Amicable pairs and aliquot cycles for elliptic curves

JOSEPH H. SILVERMAN AND KATHERINE E. STANGE

Abstract. An *amicable pair* for an elliptic curve $E/\mathbb{Q}$ is a pair of primes (p,q) of good reduction for E satisfying $\#\tilde{E}_p(\mathbb{F}_p) = q$ and $\#\tilde{E}_q(\mathbb{F}_q) = p$. In this paper we study elliptic amicable pairs and analogously defined longer *elliptic aliquot cycles*. We show that there exist elliptic curves with arbitrarily long aliqout cycles, but that CM elliptic curves (with $j \neq 0$) have no aliqout cycles of length greater than two. We give conjectural formulas for the frequency of amicable pairs. For CM curves, the derivation of precise conjectural formulas involves a detailed analysis of the values of the Grössencharacter evaluated at primes $\mathfrak{p}$ in $\mathrm{End}(E)$ having the property that $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ is prime. This is especially intricate for the family of curves with $j = 0$.

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. In this paper we study pairs of primes (p,q) such that E has good reduction at p and q and such that the reductions $\tilde{E}_p$ and $\tilde{E}_q$ of E at p and q satisfy

$$\#\tilde{E}_p(\mathbb{F}_p) = q \qquad \text{and} \qquad \#\tilde{E}_q(\mathbb{F}_q) = p.$$

By analogy with a classical problem in number theory (cf. Remark 7), we call (p,q) an *amicable pair* for the elliptic curve $E/\mathbb{Q}$.

Example 1. Searching for amicable pairs using primes smaller than 10^7 on the two elliptic curves

$$E_1 : y^2 + y = x^3 - x \quad \text{and} \quad E_2 : y^2 + y = x^3 + x^2,$$

yields one amicable pair on the curve E_1,

$$(1622311, 1622471),$$

Date: December 9, 2009, Draft #5.

1991 *Mathematics Subject Classification.* Primary: 11G05; Secondary: 11B37, 11G20, 14G25.

Key words and phrases. elliptic curve, amicable pair, aliquot cycle.

The first author's research supported by NSF DMS-0650017 and DMS-0854755. The second author's research supported by NSERC PDF-373333.

and four amicable pairs on the curve E_2,

$$(853, 883),\ (77761, 77999),\ (1147339, 1148359),\ (1447429, 1447561).$$

Example 2. The curve

$$E_3 : y^2 = x^3 + 2$$

exhibits strikingly different amicable pair behavior. There are more than 800 amicable pairs for E_3 using primes smaller that 10^6, the first few of which are

$$(13, 19), (139, 163), (541, 571), (613, 661), (757, 787), (1693, 1741).$$

One objective of this note is to present theoretical and numerical evidence for the following conjecture.

Conjecture 3. *Let $E/\mathbb{Q}$ be an elliptic curve, let*

$$\mathcal{Q}_E(X) = \#\big\{\textit{amicable pairs } (p,q) \textit{ for } E/\mathbb{Q} \textit{ with } p < q \textit{ and } p \le X\big\}.$$

be the amicable pair counting function, and assume that there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

(a) *If E does not have complex multiplication, then*

$$\mathcal{Q}_E(X) \gg\ll \frac{\sqrt{X}}{(\log X)^2} \quad \textit{as } X \to \infty,$$

where the implied constants depend on E.

(b) *If E has complex multiplication, then there is a constant $A_E > 0$ such that*

$$\mathcal{Q}_E(X) \sim A_E \frac{X}{(\log X)^2}.$$

We do not believe that it is clear, *a priori*, why there should be such a striking difference between the CM and the non-CM cases. We first discovered this phenomenon experimentally; subsequently we found an explanation based on Theorem 13, which says that if $E/\mathbb{Q}$ has CM and if $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime, then there are generally only two possible values for $\#\tilde{E}_q(\mathbb{F}_q)$, one of which is p. (The situation for $j(E) = 0$ is considerably more complicated; see Section 6.) This contrasts with the non-CM case, where $\#\tilde{E}_q(\mathbb{F}_q)$ seems to be free to range throughout the Hasse interval. We refer the reader to Conjectures 18 and 40 for more precise versions of the CM part of Conjecture 3.

The frequency of primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime or almost prime has been studied by a number of authors. In Section 1 we discuss what is known and what is conjectured concerning this problem.

Generalizing the notion of amicable pair, we define an *aliquot cycle* of length ℓ for $E/\mathbb{Q}$ to be a sequence of distinct primes $(p_1, p_2, \ldots, p_\ell)$ such that E has good reduction at every p_i and such that

$$\#\tilde{E}_{p_1}(\mathbb{F}_{p_1}) = p_2, \quad \#\tilde{E}_{p_2}(\mathbb{F}_{p_2}) = p_3, \quad \ldots \quad \#\tilde{E}_{p_{\ell-1}}(\mathbb{F}_{p_{\ell-1}}) = p_\ell, \quad \#\tilde{E}_{p_\ell}(\mathbb{F}_{p_\ell}) = p_1.$$

Example 4. The elliptic curve $y^2 = x^3 - 25x - 8$ has the aliquot triple $(83, 79, 73)$. The elliptic curve

$$E : y^2 = x^3 + 176209333661915432764478x + 60625229794681596832262$$

has an aliquot cycle $(23, 31, 41, 47, 59, 67, 73, 79, 71, 61, 53, 43, 37, 29)$ of length 14.

In Section 3 we give an heuristic argument suggesting that the counting function for aliquot cycles of length ℓ for non-CM elliptic curves grows like $\sqrt{X}/(\log X)^\ell$. The rough idea is to assume that if $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime, then the trace values $a_q(E) = q + 1 - \#\tilde{E}_q(\mathbb{F}_q)$ are (more-or-less) equidistributed within the appropriate Hasse interval.

In Section 4 we give an elementary construction (Theorem 11) using the prime number theorem, the Chinese remainder theorem, and a result of Deuring, to prove that for every ℓ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot cycle of length ℓ.

We next consider the case of elliptic curves having complex multiplication. These curves exhibit strikingly different behavior from their non-CM counterparts. Our first result (Theorem 13) says that if $E/\mathbb{Q}$ has CM with $j(E) \neq 0$, and if $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime, then there are only two possible values for $\#\tilde{E}_q(\mathbb{F}_q)$, namely p and $2q + 2 - p$. Assuming each is equally likely (which seems to be the case experimentally), this explains why CM curves have so many amicable pairs. The proof involves first proving that p and q split in $\mathrm{End}(E)$, and then relating the values of the Grössencharacter ψ_E at primes lying above p and q.

Theorem 13 can also be used to show that a CM curve with $j \neq 0$ has no aliquot cycles of length 3 or greater; see Corollary 14. This stands in contrast to Theorem 11, which says that there exist curves with arbitrarily long aliquot cycles.

We finally turn to the $j = 0$ curves $y^2 = x^3 + k$, whose complicated analysis is given in a lengthy Section 6. For prime values of k, we give a precise conjectural formula for the counting function of amicable pairs that depends on the value of k modulo 36. For example, if k is prime

and $k \equiv 1$ or $19 \pmod{36}$, then we conjecture that

$$\lim_{X\to\infty} \frac{\#\big\{p < X : p \text{ is part of an amicable pair}\big\}}{\#\big\{p < X : \#\tilde{E}_p(\mathbb{F}_p) \text{ is prime}\big\}} = \frac{1}{6} + \frac{1}{3k-9}, \quad (1)$$

while if $k \equiv 11$ or $23 \pmod{36}$, then the limiting value in (1) is (conjecturally) equal to $\frac{1}{6} + \frac{k}{3k^2-6}$. There are similar formulas for the other congruence classes.

The derivation of these formulas is in two parts. First, by analyzing the values of the Grössencharacter and using sextic reciprocity, we prove that (p, q) is an amicable pair if and only if $\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_6 \left(\frac{1-\psi_E(\mathfrak{p})}{k}\right)_6 = 1$. If the values of $\psi_E(\mathfrak{p})$ modulo k were equidistributed as p varies, we would conjecture that the number of amicable pairs is governed by the proportion of $\lambda \in \mathcal{O}/k\mathcal{O}$ satisfying $\left(\frac{\lambda(1-\lambda)}{k}\right)_6 = 1$. (Here $\mathcal{O} = \mathrm{End}(E) = \mathbb{Z}[(1+\sqrt{-3})/2]$.) This is almost true, but the allowable values of λ are often restricted by further conditions on $\left(\frac{\lambda}{k}\right)_6$. Sorting out these restrictions gives a precise conjectural value for the limit (1) in terms of the sizes of certain subsets of $\mathcal{O}/k\mathcal{O}$.

The second part of the proof is to derive explicit formulas for the sizes of these sets. This is done by relating the points in these sets to the $\mathcal{O}/k\mathcal{O}$-points on a certain family of curves $C^{(\gamma,\delta)}$ of genus four. We count these points by explicitly decomposing the Jacobian of $C^{(\gamma,\delta)}$ into a product of four $j = 0$ elliptic curves and using the Grössencharacter formula for the number of points on such curves. The resulting formulas are quite involved, especially in the case that k splits in $\mathcal{O}$, but eventually most of the terms cancel, leaving a relatively compact formula. We have no good explanation for why the final formula has such a simple form; see Remark 38 for a discussion of the delicacy of the computation.

The conjectures in this paper are supported by heuristic arguments and, especially for CM curves, by theorems describing the allowable values of the Grössencharacter ψ_E. But heuristic arguments have been known to fail, and indeed our CM argument depends on the assumption that $\psi_E(\mathfrak{p}) \bmod k$ is uniformly distributed among its *allowable values*, where we claim to have characterized the set of allowable values. It is thus reassuring that extensive experiments are in close agreement with the conjectural values derived by theory. These experiments are described in Section 7.

Finally, in Section 8 we explain where we first ran across amicable pairs and aliquot cycles for elliptic curves, and we describe some possible generalizations that deserve further study.

1. How often is $\#\tilde{E}_p(\mathbb{F}_p)$ prime?

If an elliptic curve $E/\mathbb{Q}$ is to have any amicable pairs or aliquot cycles, then it is clearly necessary that there exist primes p such that $\tilde{E}_p(\mathbb{F}_p)$ is prime. The question of existence and density of such primes has been studied by various authors.

Remark 5. If $E(\mathbb{Q})_{\text{tors}} \neq \{O\}$, then $\#\tilde{E}_p(\mathbb{F}_p)$ will be composite for all but finitely many p, since $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}_p(\mathbb{F}_p)$ for all $p \nmid 2\Delta_{E/\mathbb{Q}}$. Using this observation, it is quite easy to produce curves having no nontrivial aliquot cycles, for example, the curves $y^2 = x^3 + x$ and $y^2 = x^3 + 1$.

More generally, there may be a local obstruction associated with the representation $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(E_{\text{tors}})$ that forces $\#\tilde{E}_p(\mathbb{F}_p)$ to be composite for all but finitely many p; see [29]. We quote a special case of a conjecture of Koblitz, as modified by Zywina.

Conjecture 6. (Koblitz [9], Zywina [29]) *Let $E/\mathbb{Q}$ be an elliptic curve, and let*

$$\mathcal{N}_E(X) = \#\big\{\text{primes } p \le X \text{ such that } \#\tilde{E}_p(\mathbb{F}_p) \text{ is prime}\big\}$$

count how often E modulo p has a prime number of points. Then there is a constant $C_{E/\mathbb{Q}}$ such that

$$\mathcal{N}_E(X) \sim C_{E/\mathbb{Q}} \frac{X}{(\log X)^2}.$$

Further, $C_{E/\mathbb{Q}} > 0$ if and only if there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

Koblitz and Zywina give formulas for the constant $C_{E/\mathbb{Q}}$ in terms of the image of the representation $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(E_{\text{tors}})$. In principle this allows one to approximate $C_{E/\mathbb{Q}}$ to high precision, and they give a number of examples. For additional material on the probability that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime or almost prime, see [2] and [8].

2. Aliquot cycles and amicable pairs for elliptic curves

We formally give the following definitions as previously described in the introduction.

Definition. Let $E/\mathbb{Q}$ be an elliptic curve. An *aliquot cycle of length ℓ* for $E/\mathbb{Q}$ is a sequence of distinct primes $(p_1, p_2, \ldots, p_\ell)$ such that E has good reduction at every p_i and such that

$$\#\tilde{E}_{p_1}(\mathbb{F}_{p_1}) = p_2, \quad \#\tilde{E}_{p_2}(\mathbb{F}_{p_2}) = p_3, \quad \ldots \quad \#\tilde{E}_{p_{\ell-1}}(\mathbb{F}_{p_{\ell-1}}) = p_\ell, \quad \#\tilde{E}_{p_\ell}(\mathbb{F}_{p_\ell}) = p_1.$$

An aliquot cycle is *normalized* if $p_1 = \min p_i$. Every aliquot cycle can be normalized by a cyclic shift of its elements. An *amicable pair* is an aliquot cycle of length two.

Remark 7. Classically, an amicable pair is a pair of integers (m, n) satisfying $\tilde{\sigma}(m) = n$ and $\tilde{\sigma}(n) = m$, where $\tilde{\sigma}(n) = \sigma(n) - n$ is the sum of the proper divisors of n. Similarly, a number n is perfect if $\tilde{\sigma}(n) = n$, and a (classical) aliquot cycle is a list of distinct integers $(n_1, n_2, \ldots, n_\ell)$ satisfying

$$\tilde{\sigma}(n_1) = n_2, \quad \tilde{\sigma}(n_2) = n_3, \quad \ldots \quad \tilde{\sigma}(n_{\ell-1}) = n_\ell, \quad \tilde{\sigma}(n_\ell) = n_1.$$

(Numbers appearing in an aliquot cycle are also called sociable numbers.) Perfect numbers and amicable pairs were studied in ancient Greece, and aliquot cycles of all lengths continue to attract interest to the present day. See for example [4, 5, 25, 28].

By analogy with the classical case, one might call an aliquot cycle (p) of length one for $E/\mathbb{Q}$ a *perfect prime*, but such primes have already been given a name. They are called *anomalous primes* and appear as exceptional cases in diverse applications; see for example [12, 13]. In particular, anomalous primes are to be avoided in cryptography because the elliptic curve discrete logarithm problem (ECDLP) for anomalous primes can be solved in linear time [16, 17, 22].

We begin our study of aliquot cycles with the following general observation concerning amicable pairs.

Proposition 8. *Let $E/\mathbb{Q}$ be an elliptic curve, and let (p, q) be a normalized amicable pair for $E/\mathbb{Q}$ with $p \geq 5$. Then*

$$\mathrm{End}(\tilde{E}_p/\mathbb{F}_p) \otimes \mathbb{Q} \cong \mathrm{End}(\tilde{E}_q/\mathbb{F}_q) \otimes \mathbb{Q}.$$

Proof. The fact that p is odd and $q = \#\tilde{E}_p(\mathbb{F}_p) = p + 1 - a_p$ is prime implies in particular that $a_p \neq 0$, so E has ordinary reduction at p. (This is where we use the assumption that $p \geq 5$; cf. [20, Exercise 5.10].) Reversing the roles of p and q shows that E also has ordinary reduction at q.

The assumption that (p, q) is an amicable pair is equivalent to the assertions that

$$q = p + 1 - a_p \qquad \text{and} \qquad p = q + 1 - a_q,$$

and then a little bit of algebra shows that

$$a_p^2 - 4p = a_q^2 - 4q. \tag{2}$$

The field $\mathrm{End}(\tilde{E}_p/\mathbb{F}_p)\otimes\mathbb{Q}$ is generated by the Frobenius element $\mathrm{Frob}_p(x)=x^p$, which is a root of

$$T^2 - a_pT + p = 0.$$

Thus

$$\mathrm{End}(\tilde{E}_p/\mathbb{F}_p)\otimes\mathbb{Q} \cong \mathbb{Q}\left(\sqrt{a_p^2-4p}\,\right).$$

The analogous formula is true for q, and then (2) completes the proof of the proposition. □

3. Counting aliquot cycles for non-CM elliptic curves

In this section we study the aliquot cycle counting function

$$\mathcal{Q}_{E,\ell}(X) = \#\left\{\begin{matrix}\text{normalized aliquot cycles } (p_1,\dots,p_\ell)\\ \text{of length } \ell \text{ for } E/\mathbb{Q} \text{ satisfying } p_1 \le X\end{matrix}\right\}.$$

Conjecture 9. *Let $E/\mathbb{Q}$ be an elliptic curve that does not have complex multiplication, and assume that there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime. Then the aliquot cycle counting function satisfies*

$$\mathcal{Q}_{E,\ell}(X) \gg\ll \frac{\sqrt{X}}{(\log X)^\ell} \quad \text{as } X\to\infty,$$

where the implied positive constants depend on E and ℓ, but are independent of X.

Remark 10. As noted in Section 8, an aliquot cycle (p) of length one consists of a single anomalous prime. In this case, Conjecture 9 follows from a general conjecture of Lang and Trotter [10], which predicts the stronger result $\mathcal{Q}_{E,1}(X)\sim c\sqrt{X}/\log X$.

We give an heuristic argument in support of Conjecture 9. To ease notation, let

$$N_p = \#\tilde{E}_p(\mathbb{F}_p).$$

Then, setting $p_1=p$, we have

$$\begin{aligned}
&\mathrm{Prob}(p \text{ is part of an aliquot cycle of length } \ell)\\
&\quad= \mathrm{Prob}\left(\begin{matrix}p_2 \overset{\text{def}}{=} N_{p_1} \text{ is prime and } p_3 \overset{\text{def}}{=} N_{p_2} \text{ is prime and}\\ \dots \text{ and } p_\ell \overset{\text{def}}{=} N_{p_{\ell-1}} \text{ is prime and } N_{p_\ell}=p_1\end{matrix}\right)\\
&\quad\approx \left(\prod_{i=1}^{\ell-1}\mathrm{Prob}(p_{i+1}\overset{\text{def}}{=}N_{p_i}\text{ is prime})\right)\mathrm{Prob}(N_{p_\ell}=p_1). \qquad (3)
\end{aligned}$$

(We ignore the small probabilty that there is some $i<\ell$ such that N_{p_i} is equal to an earlier p_j.)

Under our assumption that N_p is prime for infinitely many p, Conjecture 6 says that

$$\text{Prob}(N_p \text{ is prime}) \gg\ll \frac{1}{\log p},$$

and since

$$p_{i+1} = N_{p_i} = p_i + O(\sqrt{p_i}),$$

every term in the sequence $p = p_1, p_2, \ldots, p_\ell$ satisfies $p_i = p + O(\sqrt{p})$. Hence

$$\text{Prob}(N_{p_i} \text{ is prime}) \gg\ll \frac{1}{\log p_i} \sim \frac{1}{\log p}.$$

Substituting this into (3) gives

$$\text{Prob}\begin{pmatrix} p \text{ is part of an aliquot} \\ \text{cycle of length } \ell \end{pmatrix} \approx \frac{1}{(\log p)^{\ell-1}} \cdot \text{Prob}(N_{p_\ell} = p_1). \quad (4)$$

In order to estimate the last factor, we use the Sato–Tate conjecture [20, C.21.1], which says that as q varies, the values of N_q are distributed in the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ according to the Sato–Tate distribution,

$$\#\left\{q \le X : a \le \frac{q+1-N_q}{2\sqrt{q}} \le b\right\} \sim \pi(X) \cdot \frac{2}{\pi}\int_a^b \sqrt{1-t^2}\,dt.$$

(See [24] for a proof of the Sato–Tate conjecture in certain cases, although our use of the conjecture is purely heuristic.) Then for primes p and $q = p + O(\sqrt{p})$, a rough estimate gives

$$\text{Prob}(N_q = p) \gg\ll \frac{1}{\sqrt{q}} \sim \frac{1}{\sqrt{p}}. \quad (5)$$

Combining (4) and (5) yields

$$\text{Prob}\begin{pmatrix} p \text{ is part of an aliquot} \\ \text{cycle of length } \ell \end{pmatrix} \gg\ll \frac{1}{\sqrt{p}(\log p)^{\ell-1}}.$$

We now estimate the number of normalized aliquot cycles of length ℓ whose initial prime is less than X.

$$\begin{aligned}\mathcal{Q}_{E,\ell}(X) &\approx \sum_{p\le X} \text{Prob}\begin{pmatrix} p \text{ is the initial element of a normalized} \\ \text{aliquot cycle of length } \ell \end{pmatrix} \\ &\gg\ll \sum_{p\le X} \frac{1}{\sqrt{p}(\log p)^{\ell-1}}.\end{aligned}$$

It only remains to use the rough approximation

$$\sum_{p\le X} f(X) \approx \sum_{n\le X/\log X} f(n\log n) \approx \int^{X/\log X} f(t\log t)\,dt \approx \int^{X} f(u)\,\frac{du}{\log u}$$

to obtain

$$\mathcal{Q}_{E,\ell}(X) \gg\ll \int^{X} \frac{1}{\sqrt{u}(\log u)^{\ell-1}}\cdot\frac{du}{\log u} \gg\ll \frac{\sqrt{X}}{(\log X)^{\ell}}.$$

4. Aliquot cycles of arbitrary length

Theorem 11. *For every $\ell \ge 1$ there exists an elliptic curve $E/\mathbb{Q}$ that has an aliquot cycle of length ℓ. More generally, for any positive integers $\ell_1,\dots,\ell_r$ there exists an elliptic curve $E/\mathbb{Q}$ that has distinct aliquot cycles of lengths $\ell_1,\dots,\ell_r$.*

Proof. A theorem of Deuring [3] (vastly generalized by Waterhouse [27], see also Rück [15]) says that if p is a prime and t is an integer satisfying $|t| \le 2\sqrt{p}$, then there exists an elliptic curve $\tilde{E}/\mathbb{F}_p$ satisfying

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 - t.$$

In other words, every Frobenius trace in the Hasse interval for p actually occurs as the trace of an elliptic curve defined over $\mathbb{F}_p$.

Now fix ℓ and let $p_1, p_2, \dots, p_\ell$ be a sequence of primes with the property that

$$|p_i + 1 - p_{i+1}| \le 2\sqrt{p_i} \quad \text{for all } 1 \le i \le \ell, \tag{6}$$

where by convention we set $p_{\ell+1} = p_1$. It is easy enough to find such a sequence. To be precise, we can use a weak form of the prime number theorem [1, Theorem 4.7] that says that there are positive constants a and b such that the n^{th} prime q_n satisfies

$$an\log(n) \le q_n \le bn\log(n).$$

It follows that for any given ℓ, if we choose n to be sufficiently large, then

$$q_{n+\ell} - q_n - 1 \le 2\sqrt{q_n}.$$

This implies that the sequence of primes $(q_{n+1}, q_{n+2}, \dots, q_{n+\ell})$ satisfies (6), so we take this to be our sequence $(p_1,\dots,p_\ell)$.

Applying the theorem of Deuring cited earlier, for each p_i we can find an elliptic curve $\tilde{E}_i/\mathbb{F}_{p_i}$ satisfying

$$\#\tilde{E}_i(\mathbb{F}_{p_i}) = p_{i+1}.$$

(This includes the case $i = \ell$, in which case $p_{\ell+1} = p_1$.) We now use the Chinese remainder theorem on the coefficients of the Weierstrass equations for $\tilde{E}_1, \dots, \tilde{E}_\ell$ to find an elliptic curve $E/\mathbb{Q}$ satisfying

$$E \bmod p_i \cong \tilde{E}_i \quad \text{for all } 1 \le i \le \ell.$$

Then by construction, the sequence $(p_1, \dots, p_\ell)$ is an aliquot cycle of length ℓ for $E/\mathbb{Q}$.

In a similar fashion, we can construct elliptic curves over $\mathbb{Q}$ that have aliquot cycles of any specified lengths using different sets of primes, and then we can Chinese remainder these curves to obtain a single elliptic curve over $\mathbb{Q}$ with any specified number of aliquot cycles of any specified lengths. □

Remark 12. The algorithm described in Theorem 11 works well in practice, although it naturally yields equations having large coefficients. We used it in Example 4 to find an aliquot cycle of length 14. Here's another example. The following elliptic curve has an aliquot cycle of length 25, starting with the prime $p = 41$.

$$y^2 = x^3 + 4545482133607498579268567738514832922289740324532x + 595867265462112118291430245894379464967885794713.$$

5. Amicable pairs for CM curves with $j \neq 0$

Our next goal is to formulate and provide evidence for more precise versions of the CM part of Conjecture 3. A key observation is that if E has CM, then the assumption that $q = \#\tilde{E}_p(\mathbb{F}_p)$ is prime severely limits the possible values of $\tilde{E}_q(\mathbb{F}_q)$. It turns out that the case of elliptic curves with $j(E) = 0$ is significantly more complicated than the other cases, so we deal with the $j(E) \neq 0$ curves in this section and leave the $j(E) = 0$ curves for the next section.

Theorem 13. *Let $E/\mathbb{Q}$ be an elliptic curve and assume*:

(1) *E has complex multiplication by an order $\mathcal{O}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$.*
(2) *p and q are primes of good reduction for E with $p \ge 5$ and*
$$q = \#\tilde{E}_p(\mathbb{F}_p).$$
(3) *$j(E) \neq 0$, or equivalently, $\mathcal{O} \neq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.*

Then $D \equiv 3 \pmod 4$, and either

$$\#\tilde{E}_q(\mathbb{F}_q) = p \qquad \text{or} \qquad \#\tilde{E}_q(\mathbb{F}_q) = 2q + 2 - p.$$

Theorem 13 has an interesting consequence concerning the allowable lengths of aliquot cycles for CM elliptic curves. This may be compared with Theorem 4, which says that there exist (necessarily non-CM) curves having aliqout cycles of arbitrary length, and with Conjecture 9, which implies that every non-CM elliptic curve has aliqout cycles of arbitrary length provided that there are infinitely many primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime.

Corollary 14. *A CM elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0$ has no aliquot cycles of length $\ell \geq 3$ consisting of primes $p \geq 5$.*

Remark 15. There are various ways in which one might generalize Theorem 13. For example, replacing assumption (2) by the assumption that L is an integer such that the quantity

$$q = L^2 - \big(p + 1 - \#\tilde{E}_p(\mathbb{F}_p)\big)L + p$$

is prime and splits in K leads to the following conclusion:

$$a_q(E) = \pm\big(a_p(E) + 2L\big).$$

Theorem 13 is the case $L = 1$. We omit the proof of the generalization, since it is similar and is not required in this paper.

Remark 16. Corollary 14 omits curves with $j(E) = 0$. It turns out that $j = 0$ curves possess a rich and complicated amicable pair structure which will be investigated in detail in Section 6. Corollary 24 gives an analogue of Theorem 13 saying that there are (often) six possible values for $\#\tilde{E}_q(\mathbb{F}_q)$, rather than only the two possibilities given in Theorem 13. Using this result, we are able to prove by a detailed case-by-case analysis that $j = 0$ curves cannot have aliquot cycles of length three; see Appendix A. But we do not have a proof that there are no aliquot cycles of length greater than three.

Before commencing the proofs of Theorem 13 and Corollary 14, we prove a basic result concerning the splitting of primes in CM fields.

Lemma 17. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by K, let $p \geq 5$ be a prime of good reduction for $E/\mathbb{Q}$, and suppose that $\#\tilde{E}_p(\mathbb{F}_p)$ is odd. Then p splits in K.*

Proof. We have

$$\#\tilde{E}_p(\mathbb{F}_p) = p + 1 - a_p,$$

so the assumptions that $p \neq 2$ and $\#\tilde{E}_p(\mathbb{F}_p)$ is odd imply that a_p is odd, so in particular $a_p \neq 0$. Hence E has ordinary reduction at p. (Note that our assumption that $p \geq 5$ and Hasse's bound $|a_p| \leq 2\sqrt{p}$ imply that $p \mid a_p$ if and only if $a_p = 0$.) It follows that the field K is isomorphic

to $\mathrm{End}(\tilde{E}_p)\otimes\mathbb{Q}$, which is generated by a root of the characteristic polynomial $T^2 - a_pT + p$ of Frobenius. Therefore $K = \mathbb{Q}(\sqrt{a_p^2-4p}\,)$, and

$$p = \left(\frac{a_p + \sqrt{a_p^2-4p}}{2}\right)\left(\frac{a_p - \sqrt{a_p^2-4p}}{2}\right)$$

either splits or is ramified in K. But we can rule out the latter case by noting that

$$p \text{ ramified in } K \quad\Longrightarrow\quad p \mid a_p^2 - 4p \quad\Longrightarrow\quad p \mid a_p \quad\Longrightarrow\quad a_p = 0.$$

This contradicts the fact that a_p is odd, and hence p splits in K. □

Proof of Theorem 13. Up to $\bar{\mathbb{Q}}$-isomorphism, there are 13 elliptic curves defined over $\mathbb{Q}$ that have complex multiplication. For a list, see for example [19, A §3]. There are three isomorphism classes whose conductor N_E is a power of two:

$$\begin{aligned} E &: y^2 = x^3 + x, & N_E &= 2^6,\\ E &: y^2 = x^3 + 6x^2 + x, & N_E &= 2^5,\\ E &: y^2 = x^3 + 4x^2 + 2x, & N_E &= 2^8. \end{aligned}$$

All three of these curves have a nontrivial two-torsion point, as do all of their $\bar{\mathbb{Q}}/\mathbb{Q}$ twists, so $\#E(\mathbb{F}_p)$ is even for all $p \geq 3$. Hence none of these curves admit an amicable pair; cf. Remark 5. The remaining CM curves have complex multiplication by a field $\mathbb{Q}(\sqrt{-D})$ with $D \equiv 3 \pmod 4$.

The endomorphism ring of E is an order in the field $K = \mathbb{Q}(\sqrt{-D})$, where $D \equiv 3 \pmod 4$, so it has the form

$$\mathrm{End}(E) \cong \mathcal{O} = \mathbb{Z} + f\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$$

for some integer $f \geq 1$, which is called the conductor of $\mathcal{O}$. In particular, we have $\mathcal{O}^* = \{\pm 1\}$, since our assumption that $j(E) \neq 0$ excludes the case $(D, f) = (3, 1)$.

The theory of complex multiplication says that there is a Grössencharacter ψ_E such that for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ of residue characteristic $p \geq 5$ at which E has good reduction, we have

(i) $\psi_E(\mathfrak{p}) \in \mathcal{O}$ with $\psi_E(\mathfrak{p})\mathcal{O}_K = \mathfrak{p}$.

(ii) $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) + 1 - \mathrm{Tr}\big(\psi_E(\mathfrak{p})\big)$.

See, for example, [14, Proposition 4.1] or [19, II §9]. (Note that our assumption that $\mathfrak{p}$ has residue characteristic $p \geq 5$ implies that p does not divide the conductor of $\mathcal{O}$, since our assmption that $\mathcal{O}$ has class number one implies that the conductor of $\mathcal{O}$ is at most 3.)

We are given that $p \ge 5$ and that $\#\tilde{E}_p(\mathbb{F}_p) = q$ is prime. It follows from Lemma 17 that p splits in K, say

$$p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}.$$

Then $\mathbb{F}_p = \mathbb{F}_{\mathfrak{p}}$, so

$$q = \#\tilde{E}_p(\mathbb{F}_p) = \#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = \mathrm{N}_{K/\mathbb{Q}}\big(1 - \psi_E(\mathfrak{p})\big). \tag{7}$$

Notice that this implies, in particular, that q splits in K. So writing $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, we have

$$q = \mathrm{N}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big). \tag{8}$$

Comparing (7) and (8), and using the fact that $\psi_E(\mathfrak{p})$ and $\psi_E(\mathfrak{q})$ are in $\mathcal{O}$, we see that there is a unit $u \in \mathcal{O}^*$ such that either

$$\psi_E(\mathfrak{q}) = u\big(1 - \psi_E(\mathfrak{p})\big) \qquad \text{or} \qquad \psi_E(\mathfrak{q}) = u\overline{\big(1 - \psi_E(\mathfrak{p})\big)}. \tag{9}$$

(This follows from the fact that the factorization of the ideal $q\mathcal{O}$ is unique, up to switching the factors.)

As noted earlier, we have $\mathcal{O}^* = \{\pm 1\}$, so

$$\begin{aligned}
\mathrm{Tr}\big(\psi_E(\mathfrak{q})\big) &= \pm\,\mathrm{Tr}\big(1 - \psi_E(\mathfrak{p})\big) && \text{from (9) with } u = \pm 1,\\
&= \pm\,\big(2 - \mathrm{Tr}\big(\psi_E(\mathfrak{p})\big)\big) && \text{linearity},\\
&= \pm\big(2 - (p + 1 - q)\big) && \text{since } \#\tilde{E}_p(\mathbb{F}_p) = q,\\
&= \pm(q + 1 - p).
\end{aligned}$$

Hence

$$\#\tilde{E}_q(\mathbb{F}_q) = \#\tilde{E}_{\mathfrak{q}}(\mathbb{F}_{\mathfrak{q}}) = q + 1 - \mathrm{Tr}\big(\psi_E(\mathfrak{q})\big) = q + 1 \pm (q + 1 - p).$$

This completes the proof of Theorem 13. □

Proof of Corollary 14. Let $(p_1, p_2, \ldots, p_\ell)$ be an aliquot cycle of length $\ell \ge 3$ for $E/\mathbb{Q}$ such that all $p_i \ge 5$. Since the primes in the cycle are distinct, Theorem 13 tells us that

$$p_i = 2p_{i-1} + 2 - p_{i-2} \quad \text{for } 3 \le i \le \ell.$$

Further, since the term in the aliquot sequence following p_ℓ is p_1, we have

$$p_1 = 2p_\ell + 2 - p_{\ell-1}. \tag{10}$$

Consider the linear recursion

$$A_1 = p, \quad A_2 = q, \quad A_i = 2A_{i-1} + 2 - A_{i-2} \quad \text{for } i \ge 3.$$

A simple calcuation shows that the general term of this recursion is given by the formula

$$A_i = (i-1)q - (i-2)p + (i-1)(i-2). \tag{11}$$

Hence the right-hand side of (10), which corresponds to $p_{\ell+1}$, is equal to

$$\ell p_2 - (\ell-1)p_1 + \ell(\ell-1).$$

Equating this with p_1, rearranging terms, and dividing by ℓ, yields

$$p_1 = p_2 + \ell - 1.$$

The same argument applied to the aliquot cycle

$$(p_i, p_{i+1}, \cdots, p_\ell, p_1, p_2, \ldots, p_{i-1})$$

obtained by cyclically permuting the terms in the original cycle yields

$$p_i = p_{i+1} + \ell - 1 \quad \text{for all } 1 \le i \le \ell,$$

where we set $p_{\ell+1} = p_1$. Since $\ell > 1$, this shows that $p_i > p_{i+1}$ (strict inequality). Hence

$$p_1 > p_2 > p_3 > \cdots > p_\ell > p_{\ell+1} = p_1.$$

This contradiction completes the proof of Corollary 14. □

We now use Theorem 13 to give an heuristic justification for the following conjecture.

Conjecture 18. *Let $E/\mathbb{Q}$ be an elliptic curve with with complex multiplication, and assume that $j(E) \neq 0$. Define counting functions*

$$\mathcal{N}_E(X) = \#\big\{\textit{primes } p \le X \textit{ such that } \#\tilde{E}_p(\mathbb{F}_p) \textit{ is prime}\big\},$$

$$\mathcal{Q}_E(X) = \#\big\{\textit{amicable pairs } (p,q) \textit{ for } E/\mathbb{Q} \textit{ with } p < q \textit{ and } p \le X\big\}.$$

Then either $\mathcal{N}_E(X)$ is bounded, or else

$$\lim_{X\to\infty} \frac{\mathcal{Q}_E(X)}{\mathcal{N}_E(X)} = \frac{1}{4}.$$

We note that Conjecture 6 says that if $\mathcal{N}_E(X)$ is unbounded, then it is asymptotic to $C_{E/\mathbb{Q}}X/(\log X)^2$. So the combination of Conjectures 6 and 18 gives a strengthened version of the CM part of Conjecture 3.

Our justification for Conjecture 18 is to observe that Theorem 13 says that if $\#\tilde{E}_p(\mathbb{F}_p) = q$ is prime, then there are two possibilities for $\#\tilde{E}_q(\mathbb{F}_q)$, one of which is p. Experiments indicate that each possibility occurs with equal probability, and we have no theoretical reasons for expecting otherwise, so we will accept the hypothesis that

$$\operatorname{Prob}\big(\#\tilde{E}_q(\mathbb{F}_q) = p \;\big|\; \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime}\big) = \frac{1}{2}.$$

Further, if we assume Conjecture 6, then

$$\operatorname{Prob}\big(\#\tilde{E}_p(\mathbb{F}_p) \text{ is prime} \;\big|\; p \le X\big) \sim \frac{\mathcal{N}_E(X)}{\pi(X)}.$$

Combining these estimates yields

$$\begin{aligned}
&\#\big\{p \le X : \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime and } \#\tilde{E}_q(\mathbb{F}_q) = p\big\} \\
&\qquad \approx \sum_{p\le X} \operatorname{Prob}\big(\#\tilde{E}_q(\mathbb{F}_q) = p \quad \text{and} \quad \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime}\big) \\
&\qquad \approx \sum_{p\le X} \operatorname{Prob}\big(\#\tilde{E}_q(\mathbb{F}_q) = p \;\big|\; \#\tilde{E}_p(\mathbb{F}_p) = q \text{ is prime}\big) \\
&\qquad\qquad\qquad\qquad \times \operatorname{Prob}\big(\#\tilde{E}_p(\mathbb{F}_p) \text{ is prime}\big) \\
&\qquad \approx \sum_{p\le X} \frac{1}{2} \cdot \frac{\mathcal{N}_E(X)}{\pi(X)} \\
&\qquad = \frac{\mathcal{N}_E(X)}{2}.
\end{aligned}$$

Finally, we need to divide by 2, because $\mathcal{Q}_E(X)$ only counts amicable pairs (p,q) that are normalized to satisfy $p < q$.

6. Amicable pairs for CM curves with $j = 0$

In this section we study elliptic curves having j-invariant zero. The analysis of amicable pairs on these curves is significantly more complicated than on all other CM elliptic curves, due primarily to the extra units in the endomorphism ring. In particular, experiments described in Section 7 suggest that the limiting value of $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for the curve $y^2 = x^3 + k$ varies for different values of k; see Conjecture 40.

We continue with the Grössencharacter notation from the previous section and set some additional notation that will remain in effect for this section. We let

$$\omega = \frac{1+\sqrt{-3}}{2}, \qquad K = \mathbb{Q}(\sqrt{-3}), \qquad \mathcal{O}_K = \mathbb{Z}[\omega],$$

so ω is a primitive sixth root of unity. We note that the unit group $(\mathcal{O}_K/3\mathcal{O}_K)^*$ is a group of order 6, and that the natural map

$$\boldsymbol{\mu}_6 = \mathcal{O}_K^* \xrightarrow{\sim} (\mathcal{O}_K/3\mathcal{O}_K)^*$$

is an isomorphism. Further, for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is relatively prime to 3 and any $\alpha \in \mathcal{O}_K \smallsetminus \mathfrak{p}$, we recall that the sextic residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_6$ is defined by the conditions

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_6 \in \boldsymbol{\mu}_6 \qquad \text{and} \qquad \left(\frac{\alpha}{\mathfrak{p}}\right)_6 \equiv \alpha^{\frac{1}{6}(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{p}-1)} \pmod{\mathfrak{p}}.$$

Theorem 19. *Let $k \in \mathbb{Z}$ be a nonzero integer, let $E/\mathbb{Q}$ be the elliptic curve*

$$E : y^2 = x^3 + k,$$

so E has CM by $\mathcal{O}_K$, and let ψ_E be the Grössencharacter associated to E. Suppose that $p \ge 5$ and $q \ge 5$ are primes of good reduction for E such that

$$\#\tilde{E}_p(\mathbb{F}_p) = q.$$

(a) *The prime p splits in K, say $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, and satisfies*

$$\psi_E(\mathfrak{p})\big(1 - \psi_E(\mathfrak{p})\big) \equiv 1 \pmod{3\mathcal{O}_K}.$$

(b) *The ideal defined by*

$$\mathfrak{q} = \big(1 - \psi_E(\mathfrak{p})\big)\mathcal{O}_K \quad \textit{satisfies} \quad q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}.$$

In particular, the prime q splits in K.

(c) *The values of the Grössencharacter at $\mathfrak{p}$ and $\mathfrak{q}$ are related by*

$$1 - \psi_E(\mathfrak{p}) = \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 \psi_E(\mathfrak{q}). \tag{12}$$

(d) *Let $\epsilon \in \{\pm 1\}$. Then the trace $a_q(E) = q + 1 - \#\tilde{E}_q(\mathbb{F}_q)$ satisfies*

$$a_q(E) = \epsilon(q + 1 - p) \quad \Longleftrightarrow \quad \left(\frac{4k}{\mathfrak{p}}\right)_6 \left(\frac{4k}{\mathfrak{q}}\right)_6 = \epsilon. \tag{13}$$

Remark 20. The expressions in (c) and (d) appear naturally in the course of proving Theorem 19, but we note that they may be simplified using Proposition 23, which says that $\left(\frac{4}{\mathfrak{p}}\right)_6 \left(\frac{4}{\mathfrak{q}}\right)_6 = 1$. This allows us to rewrite (12) and (13) as

$$1 - \psi_E(\mathfrak{p}) = \left(\frac{k}{\mathfrak{p}}\right)_6 \left(\frac{k}{\mathfrak{q}}\right)_6 \psi_E(\mathfrak{q}), \tag{12$'$}$$

$$a_q(E) = \pm(q + 1 - p) \quad \Longleftrightarrow \quad \left(\frac{k}{\mathfrak{p}}\right)_6 \left(\frac{k}{\mathfrak{q}}\right)_6 = \pm 1. \tag{13$'$}$$

Proof. The fact that p splits in $\mathcal{O}_K$ follows from Lemma 17, which proves the first part of (a). Next, as noted during the proof of Theorem 13, the Grössencharacter of a CM elliptic curve satisfies

$$\#\tilde{E}_p(\mathbb{F}_p) = \mathrm{N}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big) + 1 - \mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big).$$

Using the given value $q = \#\tilde{E}_p(\mathbb{F}_p)$, this can be written as

$$q = \mathrm{N}_{K/\mathbb{Q}}\big(1 - \psi_E(\mathfrak{p})\big).$$

Hence $\mathfrak{q} = \big(1 - \psi_E(\mathfrak{q})\big)\mathcal{O}_K$ satisfies $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$, which proves (b).

Further, both $\psi_E(\mathfrak{p})$ and $1 - \psi_E(\mathfrak{p})$ have norms that are relatively prime to 3. This implies first that $\psi_E(\mathfrak{p}) \equiv \omega^j \pmod 3$ for some $j \in \mathbb{Z}$, and second that j is odd, since otherwise $1 - \omega^j$ would be divisible

by $\sqrt{-3}$. On the other hand, for any odd value of j it is easy to check that

$$(1-\omega^j)\omega^j \equiv 1 \pmod{3\mathcal{O}_K},$$

so we find that

$$\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big) \equiv 1 \pmod{3\mathcal{O}_K}. \tag{14}$$

This proves the second assertion in (a).

For the proof of (c) we use the explicit formula for the Grössencharacter of curves of the form $y^2 = x^3 + k$ in terms of sextic residue symbols. This formula says that $\psi_E(\mathfrak{p}) = -\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\pi$, where the generator π is a primary generator for $\mathfrak{p}$, i.e., $\pi \equiv 2 \pmod{3\mathcal{O}_K}$. (See [7, Chapter 18, Theorem 4 and Section 7] or [14, Proposition 4.1].) Reducing this formula for ψ_E modulo 3 and applying it to both of the primes $\mathfrak{p}$ and $\mathfrak{q}$, we obtain

$$\psi_E(\mathfrak{p}) \equiv \left(\frac{4k}{\mathfrak{p}}\right)_6^{-1} \pmod{3\mathcal{O}_K} \quad \text{and} \quad \psi_E(\mathfrak{q}) \equiv \left(\frac{4k}{\mathfrak{q}}\right)_6^{-1} \pmod{3\mathcal{O}_K}. \tag{15}$$

By definition, the ideal $\mathfrak{q}$ is generated by $1-\psi_E(\mathfrak{p})$. On the other hand, the Grössencharacter has the property that $\psi_E(\mathfrak{q})$ generates the ideal $\mathfrak{q}$. It follows that there is a unit $u \in \mathcal{O}_K^* = \boldsymbol{\mu}_6$ such that $1-\psi_E(\mathfrak{p}) = u\psi_E(\mathfrak{q})$. Using (14) and (15), we find that

$$u = \frac{1-\psi_E(\mathfrak{p})}{\psi_E(\mathfrak{q})} \equiv \frac{1}{\psi_E(\mathfrak{p})\psi_E(\mathfrak{q})} \equiv \left(\frac{4k}{\mathfrak{p}}\right)_6\left(\frac{4k}{\mathfrak{q}}\right)_6 \pmod{3\mathcal{O}_K}.$$

Since a sixth root of unity is determined by its residue modulo 3, this last congruence is an equality, which completes the proof of (c).

Using the defining property of the Grössencharacter and formula (12) from (c), we have

$$a_q(E) = \mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\left(\frac{4k}{\mathfrak{q}}\right)_6^{-1}\big(1-\psi_E(\mathfrak{p})\big)\right).$$

Similarly, using the assumption that $\#\tilde{E}_p(\mathbb{F}_p) = q$, we find that

$$\mathrm{Tr}_{E/\mathbb{Q}}\big(1-\psi_E(\mathfrak{p})\big) = 2 - \mathrm{Tr}_{E/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big) = 2-(p+1-q) = q+1-p.$$

Hence for $\epsilon \in \{\pm 1\}$, we have

$$a_q(E) = \epsilon(q+1-p) \quad \Longleftrightarrow$$
$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\epsilon\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\left(\frac{4k}{\mathfrak{q}}\right)_6^{-1}\big(1-\psi_E(\mathfrak{p})\big)\right) = \mathrm{Tr}_{E/\mathbb{Q}}\big(1-\psi_E(\mathfrak{p})\big).$$

We now use the following lemma, which may be applied because the quantity $\mathrm{N}_{E/\mathbb{Q}}\big(1-\psi_E(\mathfrak{p})\big) = q$ is neither a square nor 3 times a square. The lemma allows us to conclude that

$$a_q(E) = \epsilon(q+1-p) \quad \Longleftrightarrow \quad \epsilon\left(\frac{4k}{\mathfrak{p}}\right)_6^{-1}\left(\frac{4k}{\mathfrak{q}}\right)_6^{-1} = 1,$$

which completes the proof of (e). □

Lemma 21. *Let $\alpha \in \mathcal{O}_K$ have the property the $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ is neither a square nor 3 times a square. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \quad \textit{with } \zeta \in \boldsymbol{\mu}_6 \quad \Longleftrightarrow \quad \zeta = 1.$$

Proof. We have

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}}(\zeta\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \quad &\Longleftrightarrow \quad \mathrm{Tr}_{K/\mathbb{Q}}\big((\zeta-1)\alpha\big) = 0 \\
&\Longleftrightarrow \quad (\zeta-1)\alpha = c\sqrt{-3} \text{ for some } c \in \mathbb{Z}, \\
&\Longleftrightarrow \quad \zeta = 1 \text{ or } \alpha = c\frac{\sqrt{-3}}{\zeta-1}.
\end{aligned}$$

(Note that c is in $\mathbb{Z}$ because ζ and α are in $\mathcal{O}_K = \mathbb{Z}[\omega]$.) Suppose that $\zeta \neq 1$. We observe that as ζ ranges over $\boldsymbol{\mu}_6 \smallsetminus \{1\}$, the quantity $\sqrt{-3}/(\zeta-1)$ takes on the five values

$$\left\{2-\omega, 1-\omega, \frac{1}{2}-\omega, -\omega, -1-\omega\right\}.$$

The norms of these five numbers form the set $\{1, 3, \frac{3}{4}\}$, so the norm of α would have the form c^2, $3c^2$, or $3(c/2)^2$, contradicting the assumption on $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$. □

We can use Theorem 19 to show that for some curves with $j(E) = 0$, the conclusion of Theorem 13 is true, i.e., there are only two possible values for $\#\tilde{E}_q(\mathbb{F}_q)$.

Corollary 22. *Let $d \in \mathbb{Z}$ be a nonzero integer, and let E be the elliptic curve $E : y^2 = x^3 + 2d^3$. Let p be a prime with $p \nmid 6d$ such that $q = \#\tilde{E}_p(\mathbb{F}_p)$ is also prime and satisfies $q \nmid 6d$. Then*

$$\#\tilde{E}_q(\mathbb{F}_q) = p \qquad \textit{or} \qquad \#\tilde{E}_q(\mathbb{F}_q) = 2q+2-p.$$

Proof. Using notation from Theorem 19, we have $k = 2d^3$, so

$$\left(\frac{4k}{\mathfrak{p}}\right)_6 = \left(\frac{2d}{\mathfrak{p}}\right)_6^3 = \pm 1 \quad \text{and} \quad \left(\frac{4k}{\mathfrak{q}}\right)_6 = \left(\frac{2d}{\mathfrak{q}}\right)_6^3 = \pm 1.$$

It follows from Theorem 19(d) that $a_q(E) = \pm(q+1-p)$. □

We next prove two useful facts.

Proposition 23. *Let k, E, p, q, $\mathfrak{p}$, and $\mathfrak{q}$ be as in the statement of Theorem 19.*

(a) $\left(\dfrac{k}{\mathfrak{p}}\right)_6 = \omega \quad or \quad \omega^5$.

(b) $\left(\dfrac{2}{\mathfrak{p}}\right)_6\left(\dfrac{2}{\mathfrak{q}}\right)_6 = \left(\dfrac{2}{p}\right)_{\mathbb{Q}}\left(\dfrac{2}{q}\right)_{\mathbb{Q}}$, *so in particular,* $\left(\dfrac{2}{\mathfrak{p}}\right)_6\left(\dfrac{2}{\mathfrak{q}}\right)_6 = \pm 1$.

(*In* (b), $\left(\frac{\cdot}{\cdot}\right)_{\mathbb{Q}}$ *denotes the usual quadratic residue symbol in* $\mathbb{Z}$.)

Proof. (a) If k is a square modulo $\mathfrak{p}$, then $\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ has a nontrivial 3-torsion point, so $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ cannot be prime. Similarly, if k is a cube modulo $\mathfrak{p}$, then $\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ has a nontrivial 2-torsion point, so again $\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ cannot prime. Hence

$$\left(\frac{k}{\mathfrak{p}}\right)_6^3 = \left(\frac{k}{\mathfrak{p}}\right)_2 \neq 1 \qquad \text{and} \qquad \left(\frac{k}{\mathfrak{p}}\right)_6^2 = \left(\frac{k}{\mathfrak{p}}\right)_3 \neq 1.$$

This means that $\left(\frac{k}{\mathfrak{p}}\right)_6$ cannot equal 1, ω^2, ω^3, or ω^4, so it must be either ω or ω^5.

(b) We first note that for any $\alpha, \beta \in \mathcal{O}_K$ with $\gcd(6, \beta) = 1$, we have

$$\left(\frac{\alpha}{\beta}\right)_6^{-1} = \left(\frac{\alpha}{\beta}\right)_6^5 = \left(\frac{\alpha}{\beta}\right)_6^3\left(\frac{\alpha}{\beta}\right)_6^2 = \left(\frac{\alpha}{\beta}\right)_2\left(\frac{\alpha}{\beta}\right)_3. \tag{16}$$

If, in addition, $\alpha \in \mathbb{Z}$, then [7, Chapter 18, Section 7, Lemma 2] says that $\left(\frac{\alpha}{\beta}\right)_2 = \left(\frac{\alpha}{\mathrm{N}_{K/\mathbb{Q}}(\beta)}\right)_{\mathbb{Q}}$.

In order to prove (b), we use cubic reciprocity [7, Chapter 9, Section 3]. We recall that an element $\alpha \in \mathcal{O}_K$ is said to be *primary* if $\alpha \equiv 2 \pmod{3\mathcal{O}_K}$. Since $\psi_E(\mathfrak{p})$ is relatively prime to 3, there is a (unique) sixth root of unity $\zeta \in \boldsymbol{\mu}_6$ such that $\zeta\psi_E(\mathfrak{p})$ is primary. It follows from Theorem 19(a) that $\zeta^{-1}\big(1 - \psi_E(\mathfrak{p})\big)$ is also primary, and of course, the number 2 is primary. Hence cubic reciprocity yields

$$\begin{aligned}
\left(\frac{2}{\mathfrak{p}}\right)_3\left(\frac{2}{\mathfrak{q}}\right)_3 &= \left(\frac{2}{\psi_E(\mathfrak{p})}\right)_3\left(\frac{2}{1-\psi_E(\mathfrak{p})}\right)_3 \\
&= \left(\frac{2}{\zeta\psi_E(\mathfrak{p})}\right)_3\left(\frac{2}{\zeta^{-1}(1-\psi_E(\mathfrak{p}))}\right)_3 \\
&= \left(\frac{\zeta\psi_E(\mathfrak{p})}{2}\right)_3\left(\frac{\zeta^{-1}(1-\psi_E(\mathfrak{p}))}{2}\right)_3 \\
&= \left(\frac{\psi_E(\mathfrak{p})(1-\psi_E(\mathfrak{p}))}{2}\right)_3.
\end{aligned} \tag{17}$$

The primes $\psi_E(\mathfrak{p})$ and $1-\psi_E(\mathfrak{p})$ are relatively prime to 2, so $\psi_E(\mathfrak{p})$ is congruent to either ω or $1+\omega$ modulo 2. (Note that $\mathcal{O}_K/2\mathcal{O}_K = \{0,1,\omega,1+\omega\}$.) Hence

$$\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big) \equiv \omega(1+\omega) \equiv 1 \pmod{2\mathcal{O}_K}.$$

Substituting into (17) shows that $\left(\frac{2}{\mathfrak{p}}\right)_3\left(\frac{2}{\mathfrak{q}}\right)_3 = 1$. Using (16) and its accompanying remark, we find that

$$\left(\frac{2}{\mathfrak{p}}\right)_6^{-1}\left(\frac{2}{\mathfrak{q}}\right)_6^{-1} = \left(\frac{2}{\mathfrak{p}}\right)_2\left(\frac{2}{\mathfrak{q}}\right)_2\left(\frac{2}{\mathfrak{p}}\right)_3\left(\frac{2}{\mathfrak{q}}\right)_3 = \left(\frac{2}{p}\right)_{\mathbb{Q}}\left(\frac{2}{q}\right)_{\mathbb{Q}},$$

which completes the proof of (b). □

Corollary 24. *Let $E/\mathbb{Q}$, p, and q be as in the statement of Theorem 19.*

(a) *There exists an integer A satisfying*

$$A^2 = \frac{2pq+2p+2q-p^2-q^2-1}{3}. \tag{18}$$

(b) *The trace $a_q(E) = q+1-\#\tilde{E}_q(\mathbb{F}_q)$ equals one of the following six values*:

$$\pm\,(q+1-p), \quad \frac{\pm(q+1-p)\pm 3A}{2}. \tag{19}$$

Remark 25. The six possible values of $\#\tilde{E}_q(\mathbb{F}_q)$ described in Corollary 24(b) are $\#\tilde{E}_q^{(d)}(\mathbb{F}_q)$ for the sextic twists of $\tilde{E}_q$ corresponding to the elements of $H^1\big(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}(\tilde{E}_q)\big) \cong H^1\big(\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q), \boldsymbol{\mu}_6\big) \cong \mathbb{F}_q^*/(\mathbb{F}_q^*)^6$.

Remark 26. Using Corollary 24 and a case-by-case analysis, we prove in Appendix A that $j=0$ elliptic curves have no aliquot cycles of length three.

Proof. (a) We know that $\mathrm{Tr}\big(\psi_E(\mathfrak{p})\big) = a_p(E)$, so writing $\psi_E(\mathfrak{p})$ as an element of $\mathcal{O}_K = \mathbb{Z}[\omega]$, it has the form

$$\psi_E(\mathfrak{p}) = \frac{a_p(E) + A\sqrt{-3}}{2} \quad \text{for some } A \in \mathbb{Z}. \tag{20}$$

Since we also know that $\mathrm{N}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{p})\big) = p$, we find that

$$\frac{a_p(E)^2 + 3A^2}{4} = p. \tag{21}$$

Finally, the assumption that $\#\tilde{E}_p(\mathbb{F}_p) = q$ is equivalent to $a_p(E) = p+1-q$. Substituting this value into (21), a little bit of algebra shows that A has the form specified by (18).

(b) Applying (12) from Theorem 19, we find that

$$\mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big) = \mathrm{Tr}_{K/\mathbb{Q}}\big(\zeta(1-\psi_E(\mathfrak{p}))\big)$$

for some $\zeta \in \boldsymbol{\mu}_6$. Using the value of $\psi_E(\mathfrak{p})$ from (20) with the substitution $a_p(E) = p+1-q$ yields

$$\mathrm{Tr}_{K/\mathbb{Q}}\big(\psi_E(\mathfrak{q})\big) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\zeta\left(\frac{q+1-p-A\sqrt{-3}}{2}\right)\right).$$

Substituting in each of the six possible values $\zeta \in \boldsymbol{\mu}_6$ and taking the trace yields the six values listed in (19). □

Definition. Fix a non $E : y^2 = x^3 + k$. We let $\mathcal{N}_k$ denote the set

$$\mathcal{N}_k = \left\{\begin{matrix}\text{primes } p \ge 5 \text{ of good reduction for } E\\ \text{such that } q = \#\tilde{E}_p(\mathbb{F}_p) \text{ is also}\\ \text{a prime of good reduction for } E\end{matrix}\right\}.$$

(This differs slightly from our earlier notation in that we are now excluding a few primes, but this does not affect our asymptotic formulas.) We define a subset of $\mathcal{N}_k$ by

$$\mathcal{N}_k^{[1]} = \big\{p \in \mathcal{N}_k : a_q(E) = \pm(q+1-p)\big\},$$

and we say that the primes in $\mathcal{N}_k^{[1]}$ are of Type 1 for E. We write $\mathcal{N}_k(X)$ for the number of primes in $\mathcal{N}_k$ that are less than X, and similarly for $\mathcal{N}_k^{[1]}(X)$.

Only Type 1 primes can be amicable, and based on experiments, we expect that about half of the Type 1 primes will be part of an amicable pair. Let

$$\mathcal{Q}_k(X) = \#\big\{p < X : p < q \text{ and } (p,q) \text{ is an amicable pair for } E\big\},$$

i.e., $\mathcal{Q}_k(X)$ is the number of normalized amicable pairs (p,q) on E with $p < X$. Then we have the following conjecture, where the conjectured limit is $\frac{1}{4}$, rather than $\frac{1}{2}$, because $\mathcal{Q}_k(X)$ counts amicable pairs (p,q) with $p<q$, while $\mathcal{N}_k^{[1]}(X)$ counts both (p,q) and (q,p).

Conjecture 27. *With notation as above, the proportion of Type* 1 *primes that are part of a normalized amicable pair is given by*

$$\lim_{X\to\infty} \frac{\mathcal{Q}_k(X)}{\mathcal{N}_k^{[1]}(X)} = \frac{1}{4}.$$

Thus in order to understand the distribution of amicable pairs on E, we need to study the density of the Type 1 primes in $\mathcal{N}_k$.

Remark 28. According to Corollary 24, there are six possible values for $a_q(E)$, two of which give Type 1 primes, so one might expect $\mathcal{N}_k^{[1]}$ to have density $\frac{1}{3}$ inside $\mathcal{N}_k$. This turns out not to be the case. At the extreme end, Corollary 22 says that $\mathcal{N}_{2d^3}^{[1]} = \mathcal{N}_{2d^3}$ for any nonzero $d \in \mathbb{Z}$. The rest of this section is devoted to developing tools for calculating a conjectural value for $\lim_{X\to\infty} \mathcal{N}_k^{[1]}(X)/\mathcal{N}_k(X)$. This value depends on k in quite a complicated way; see Conjecture 30. For precise formulas when k is prime, see Conjecture 40, which says that the limit should equal $\frac{1}{3} + R(k)$, where $R(k)$ is a rational function of k that depends on k modulo 36.

Definition. We set the notation

$$n \overset{pr}{\equiv} a \pmod{m} \quad \Longleftrightarrow \quad p \equiv a \pmod{m} \text{ for every prime } p \mid n.$$

Further, for any ideal $\mathfrak{K} \subset \mathcal{O}_K$ we define

$$\mathcal{O}_{K,\mathfrak{K}}^\sharp = \left\{ \lambda \in \frac{\mathcal{O}_K}{\mathfrak{K}} : \gcd\big(\lambda(1-\lambda), \mathfrak{K}\big) = 1 \right\}.$$

If $\mathfrak{K} = k\mathcal{O}_K$ is principal, we write simply $\mathcal{O}_{K,k}^\sharp$.

Now let $k \in \mathbb{Z}$ satisfy $\gcd(6,k) = 1$. We define a set M_k that depends on k modulo 4 and on the primes dividing k modulo 9.

(a) $k \equiv 1 \pmod 4$ and $k \overset{pr}{\equiv} \pm 1 \pmod 9$

$$M_k = \left\{ \lambda \in \mathcal{O}_{K,k}^\sharp : \left(\frac{\lambda}{k}\right)_2 = -1 \text{ and } \left(\frac{\lambda}{k}\right)_3 \neq 1 \right\}.$$

(b) $k \equiv 1 \pmod 4$ and $k \overset{pr}{\not\equiv} \pm 1 \pmod 9$

$$M_k = \left\{ \lambda \in \mathcal{O}_{K,k}^\sharp : \left(\frac{\lambda}{k}\right)_2 = -1 \right\}.$$

(c) $k \equiv 3 \pmod 4$ and $k \overset{pr}{\equiv} \pm 1 \pmod 9$

$$M_k = \left\{ \lambda \in \mathcal{O}_{K,k}^\sharp : \left(\frac{\lambda}{k}\right)_3 \neq 1 \right\}.$$

(d) $k \equiv 3 \pmod 4$ and $k \overset{pr}{\not\equiv} \pm 1 \pmod 9$

$$M_k = \mathcal{O}_{K,k}^\sharp.$$

Further, for every k we define a subset of M_k by

$$M_k^{[1]} = \left\{ \lambda \in M_k : \left(\frac{\lambda(1-\lambda)}{k}\right)_3 = 1 \right\}.$$

k	$\#\mathcal{O}_{K,k}^\sharp$	$\#M_k$	$\#M_k^{[1]}$	$\#M_k^{[1]}/\#M_k$
37 (a.1)	1225	408	144	$\frac{6}{17} = 0.3529$
17 (a.2)	287	96	36	$\frac{3}{8} = 0.3750$
13 (b.1)	121	60	20	$\frac{1}{3} = 0.3333$
5 (b.2)	23	12	4	$\frac{1}{3} = 0.3333$
19 (c.1)	289	192	72	$\frac{3}{8} = 0.3750$
71 (c.2)	5039	3360	1152	$\frac{12}{35} = 0.3429$
7 (d.1)	25	25	13	$\frac{13}{25} = 0.5200$
11 (d.2)	119	119	47	$\frac{47}{119} = 0.3950$

TABLE 1. The sets $\mathcal{O}_{K,k}^\sharp$, M_k and $M_k^{[1]}$

Remark 29. It is easy to check that $k \overset{pr}{\equiv} \pm 1 \pmod 9$ if and only if every cube root of unity in $\mathcal{O}_K/k\mathcal{O}_K$ is itself a cube. For example, suppose that $k \in \mathbb{Z}$ is prime. If $k \equiv -1 \pmod 9$, then $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_{k^2}$ is a finite field with k^2 elements, and $\boldsymbol{\mu}_9 \subset \mathbb{F}_{k^2}$. Similarly, if $k \equiv 1 \pmod 9$, then $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_k \times \mathbb{F}_k$, and $\boldsymbol{\mu}_9 \subset \mathbb{F}_k$. Thus in both cases, every cube root of unity in $\mathcal{O}_K/k\mathcal{O}_K$ is itself a cube.

Conjecture 30. *Let $k \in \mathbb{Z}$ be an integer satisfying* $\gcd(6,k) = 1$. *Then*

$$\lim_{X\to\infty} \frac{\mathcal{N}_k^{[1]}(X)}{\mathcal{N}_k(X)} = \frac{\#\mathcal{M}_k^{[1]}}{\#\mathcal{M}_k}. \tag{22}$$

Remark 31. For small values of k it is not difficult to compute the sets $\mathcal{M}_k$ and $\mathcal{M}_k^{[1]}$, thereby obtaining an explicit (conjectural) value for the limit (22). Table 1 gives some examples corresponding to the four cases (a)–(d) used to define $\mathcal{M}_k$, further divided according to the value of k modulo 3. (The notation $(x.n)$ after each value of k indicates the case $x =$ (a),...,(d) and the congruence class $k \equiv n \pmod 3$.)

Our justification for Conjecture 30 uses the following weak form of quadratic and cubic reciprocity for the field $\mathbb{Q}(\omega)$.

Lemma 32. *Let $k \in \mathbb{Z}$ satisfy* $\gcd(k,6) = 1$, *and let $\lambda \in \mathbb{Z}[\omega]$ satisfy* $\gcd(6k,\lambda) = 1$.

(a) (Quadratic Reciprocity in $\mathbb{Q}(\omega)$)

$$\left(\frac{k}{\lambda}\right)_2 = (-1)^{\frac{\mathrm{N}(\lambda)-1}{2}\cdot\frac{k-1}{2}} \left(\frac{\lambda}{k}\right)_2.$$

(b) (Cubic Reciprocity in $\mathbb{Q}(\omega)$) *Let $\zeta \in \boldsymbol{\mu}_3$ be the unique cube root of unity such that*

$$\zeta\lambda \equiv \pm 1 \pmod{3\mathcal{O}_K}.$$

Then

$$\left(\frac{k}{\lambda}\right)_3 = \left(\frac{\zeta}{k}\right)_3 \left(\frac{\lambda}{k}\right)_3.$$

Proof. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ satisfy $\gcd(\alpha, \beta) = \gcd(\alpha\beta, 6) = 1$. We start with the sextic reciprocity law for $\mathbb{Q}(\omega)$ as stated in [11, Theorem 7.10]. This says that if α and β are "E-primary" (see [11] for terminology), then

$$\left(\frac{\alpha}{\beta}\right)_6 \left(\frac{\beta}{\alpha}\right)_6^{-1} = (-1)^{\frac{\mathrm{N}(\alpha)-1}{2}\cdot\frac{\mathrm{N}(\beta)-1}{2}}. \tag{23}$$

Let $\rho = \omega^2$ denote a primitive cube root of unity. Then for $\alpha \in \mathcal{O}_K$ satisfying $\gcd(6, \alpha) = 1$, we have by definition

$$\alpha \text{ is } E\text{-primary} \iff \begin{cases} \alpha \equiv \pm 1 \pmod 3 \text{ and} \\ \alpha^3 = A + B\rho \text{ with } A + B \equiv 1 \pmod 4. \end{cases}$$

(This is a corrected version of [11, Lemma 7.9], which omits the $\alpha \equiv \pm 1 \pmod 3$ condition and includes a superfluous $3 \mid B$ requirement.) We note that if $\alpha \equiv \pm 1 \pmod 3$, then exactly one of $\pm\alpha$ is E-primary.

We now consider $k \in \mathbb{Z}$ and $\lambda \in \mathcal{O}_K$ as in the statement of the lemma. Since k is an integer and satisfies $\gcd(6, k) = 1$, we have

$$\begin{aligned} k \text{ is } E\text{-primary} &\iff k \equiv \pm 1 \pmod 3 \quad \text{and} \quad k^3 \equiv 1 \pmod 4 \\ &\iff k \equiv 1 \pmod 4, \end{aligned}$$

so $(-1)^{(k-1)/2}k$ is E-primary. We also note that for any $\alpha \in \mathcal{O}_K$ satisfying $\gcd(6, \alpha) = 1$, Euler's formula says that

$$\left(\frac{-1}{\alpha}\right)_6 \equiv (-1)^{\frac{\mathrm{N}(\alpha)-1}{6}} \pmod{\alpha\mathcal{O}_K}, \tag{24}$$

and since both sides of (24) are sixth roots of unity, the congruence (24) is an equality. In particular,

$$\left(\frac{-1}{k}\right)_6 = (-1)^{\frac{\mathrm{N}(k)-1}{6}} = (-1)^{\frac{k^2-1}{6}} = 1. \tag{25}$$

It is an easy exercise to verify that there is a unique $\zeta \in \boldsymbol{\mu}_3$ such that $\zeta\lambda \equiv \pm 1 \pmod 3$, cf. [7, Chapter 9, Proposition 9.3.5]. Then one

of $\pm\zeta\lambda$ is E-primary, so we can apply (23) to the E-primary numbers $\alpha = (-1)^{(k-1)/2}k$ and $\beta = \pm\zeta\lambda$. Then (23) becomes

$$\left(\frac{(-1)^{(k-1)/2}k}{\lambda}\right)_6 \left(\frac{\pm\zeta\lambda}{k}\right)_6^{-1} = (-1)^{\frac{k^2-1}{2}\cdot\frac{\mathrm{N}(\lambda)-1}{2}} = 1.$$

(The second equality comes from the fact that $k^2 \equiv 1 \pmod 4$.) Hence

$$\left(\frac{-1}{\lambda}\right)_6^{(k-1)/2} \left(\frac{k}{\lambda}\right)_6 \left(\frac{\pm1}{k}\right)_6^{-1} \left(\frac{\zeta}{k}\right)_6^{-1} \left(\frac{\lambda}{k}\right)_6^{-1} = 1.$$

Using (24) and (25) gives

$$\left(\frac{k}{\lambda}\right)_6 = (-1)^{\frac{\mathrm{N}(\lambda)-1}{2}\cdot\frac{k-1}{2}} \left(\frac{\zeta}{k}\right)_6 \left(\frac{\lambda}{k}\right)_6. \tag{26}$$

(We note in particular that the sign used to ensure that $\zeta\lambda$ is E-primary turns out to be irrelevant because $\left(\frac{-1}{k}\right)_6 = 1$.) Cubing (26) and using $\zeta^3 = 1$ gives the quadratic reciprocity formula in (a), and similarly squaring (26) gives the cubic reciprocity formula in (b). □

Justification for Conjecture 30. Let $p \in \mathcal{N}_k$, so Theorem 19(a) tells us that p splits in $\mathcal{O}_K$, say $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. As in that theorem, we let $\mathfrak{q} = \big(1 - \psi_E(\mathfrak{p})\big)\mathcal{O}_K$. Then squaring Theorem 19(d) yields

$$p \in \mathcal{N}_k^{[1]} \quad\Longleftrightarrow\quad \left(\frac{4k}{\mathfrak{p}}\right)_3 \left(\frac{4k}{\mathfrak{q}}\right)_3 = 1.$$

Further, Proposition 23 implies that $\left(\frac{2}{\mathfrak{p}}\right)_3 \left(\frac{2}{\mathfrak{q}}\right)_3 = 1$, so we find that

$$p \in \mathcal{N}_k^{[1]} \quad\Longleftrightarrow\quad \left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = 1.$$

The (prime) ideals $\mathfrak{p}$ and $\mathfrak{q}$ are generated, respectively, by the elements $\psi_E(\mathfrak{p})$ and $1-\psi_E(\mathfrak{p})$, and Theorem 19(a) says that these elements satisfy

$$\psi_E(\mathfrak{p})\big(1 - \psi_E(\mathfrak{p})\big) \equiv 1 \pmod{3\mathcal{O}_K}. \tag{27}$$

Hence if we choose $\xi \in \boldsymbol{\mu}_6$ to satisfy

$$\xi\psi_E(\mathfrak{p}) \equiv \pm1 \pmod{3\mathcal{O}_K},$$

then (27) says that we also have

$$\xi^{-1}\big(1 - \psi_E(\mathfrak{p})\big) \equiv \pm1 \pmod{3\mathcal{O}_K}.$$

This allow us to apply cubic reciprocity (Lemma 32(b), or [7, Chapter 9, Section 3, Theorem 1]) to compute

$$\left(\frac{k}{\mathfrak{p}}\right)_3 \left(\frac{k}{\mathfrak{q}}\right)_3 = \left(\frac{k}{\xi\psi_E(\mathfrak{p})\mathcal{O}_K}\right)_3 \left(\frac{k}{\xi^{-1}(1-\psi_E(\mathfrak{p}))\mathcal{O}_K}\right)_3$$

$$= \left(\frac{\xi\psi_E(\mathfrak{p})}{k\mathcal{O}_K}\right)_3 \left(\frac{\xi^{-1}(1-\psi_E(\mathfrak{p}))}{k\mathcal{O}_K}\right)_3$$
$$= \left(\frac{\psi_E(\mathfrak{p})}{k\mathcal{O}_K}\right)_3 \left(\frac{1-\psi_E(\mathfrak{p})}{k\mathcal{O}_K}\right)_3.$$

Hence

$$p \in \mathcal{N}_k^{[1]} \quad \Longleftrightarrow \quad \left(\frac{\psi_E(\mathfrak{p})\big(1-\psi_E(\mathfrak{p})\big)}{k\mathcal{O}_K}\right)_3 = 1. \tag{28}$$

We now consider how the values $\psi_E(\mathfrak{p})$ are distributed in $\mathcal{O}_K/k\mathcal{O}_K$ as p varies in $\mathcal{N}_k$. If p were chosen completely randomly,subject only to $p \equiv 1 \pmod 3$, then we might expect the values of $\psi_E(\mathfrak{p})$ to be uniformly distributed among the congruence classes in $\mathcal{O}_K/k\mathcal{O}_K$. However, Proposition 24(a) tells us that $\left(\frac{k}{\mathfrak{p}}\right)_6$ equals either ω or ω^5, i.e., it is a primitive sixth root of unity. Equivalently,

$$\left(\frac{k}{\mathfrak{p}}\right)_2 = -1 \qquad \text{and} \qquad \left(\frac{k}{\mathfrak{p}}\right)_3 = \omega^2 \text{ or } \omega^4, \tag{29}$$

i.e., neither $\left(\frac{k}{\mathfrak{p}}\right)_2$ nor $\left(\frac{k}{\mathfrak{p}}\right)_3$ equals 1. This gives a constraint on the values of $\psi_E(\mathfrak{p})$ for $p \in \mathcal{N}_k$. Discarding finitely many elements of $\mathcal{N}_k$, we may assume that $p \nmid 6k$, and then reciprocity (Lemma 32) tells us that

$$\left(\frac{k}{\mathfrak{p}}\right)_2 = (-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}} \left(\frac{\psi_E(\mathfrak{p})}{k}\right)_2 \qquad \text{and} \qquad \left(\frac{k}{\mathfrak{p}}\right)_3 = \left(\frac{\zeta}{k}\right)_3 \left(\frac{\psi_E(\mathfrak{p})}{k}\right)_3,$$

where $\zeta \in \boldsymbol{\mu}_3$ satisfies $\zeta\psi_E(\mathfrak{p}) \equiv \pm 1 \pmod 3$. (Note that $\mathrm{N}\big(\psi_E(\mathfrak{p})\big) = p$.) Hence the constraints (29) on $\psi_E(\mathfrak{p})$ from Proposition 24(a) become

$$\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_2 = -(-1)^{\frac{p-1}{2}\cdot\frac{k-1}{2}} \qquad \text{and} \qquad \left(\frac{\zeta}{k}\right)_3 \left(\frac{\psi_E(\mathfrak{p})}{k}\right)_3 = \omega^2 \text{ or } \omega^4. \tag{30}$$

We now make the following two assumptions, which are supported by experiments:

- For $p \in \mathcal{N}_k$, the value of $p \bmod 4$ is equally likely to be 1 or 3.
- For $p \in \mathcal{N}_k$, the value of ζ in (30) is equally likely to be 1, ω^2, or ω^4.

These assumptions have the following consequences:

- If $k \equiv 3 \pmod 4$, then the first equation in (30) has no effect on the value of $\psi_E(\mathfrak{p}) \bmod k$.
- If $k \overset{pr}{\not\equiv} \pm 1 \pmod 9$, i.e., if cube roots of unity in $\mathcal{O}_K/k\mathcal{O}_K$ are not necessarily cubes, then the second equation in (30) has no effect on the value of $\psi_E(\mathfrak{p}) \bmod k$.

On the other hand, if $k \equiv 1 \pmod 4$, then the first equation in (30) gives the constraint $\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_2 = -1$; and similarly, if $k \overset{pr}{\equiv} \pm 1 \pmod 9$, then the second equation in (30) imposes the condition $\left(\frac{\psi_E(\mathfrak{p})}{k}\right)_3 \neq 1$. Thus considering the four cases, we see that $\psi_E(\mathfrak{p})$ is in the set M_k. Further, we note that (28) says that $p \in \mathcal{N}_k^{[1]}$ if and only if $\psi_E(\mathfrak{p}) \in \mathcal{M}_k^{[1]}$. Hence it is reasonable to conjecture that the density of $\mathcal{N}_k^{[1]}$ in $\mathcal{N}_k$ is given by the ratio $\#\mathcal{M}_k^{[1]}/\#\mathcal{M}_k$. □

Conjecture 30 is reasonably satisfactory in that the sets $\mathcal{M}_k$ and $\mathcal{M}_k^{[1]}$ are easy to compute for any particular (not-too-large) value of k. In the remainder of this section we derive explicit formulas for $\#\mathcal{M}_k$ and $\#\mathcal{M}_k^{[1]}$ when k is prime. We do this by breaking them up into subsets of the following sort. For any ideal $\mathfrak{K} \subset \mathcal{O}_K$ and any roots of unity $\zeta \in \boldsymbol{\mu}_6$ and $\xi \in \boldsymbol{\mu}_3$, we define

$$\begin{aligned} M_{\mathfrak{K}}(\zeta) &= \left\{ \lambda \in \mathcal{O}_{K,\mathfrak{K}}^\sharp : \left(\frac{\lambda}{\mathfrak{K}}\right)_6 = \zeta \right\} \\ &= \left\{ \lambda \in \mathcal{O}_{K,\mathfrak{K}}^\sharp : \left(\frac{\lambda}{\mathfrak{K}}\right)_2 = \zeta^3 \text{ and } \left(\frac{\lambda}{\mathfrak{K}}\right)_3 = \zeta^2 \right\}, \\ M_{\mathfrak{K}}^{[1]}(\zeta,\xi) &= \left\{ \lambda \in M_{\mathfrak{K}}(\zeta) : \left(\frac{\lambda(1-\lambda)}{\mathfrak{K}}\right)_3 = \xi \right\}. \end{aligned}$$

As before, if $\mathfrak{K} = k\mathcal{O}_K$ is principal, we write $M_k(\zeta)$ and $M_k^{[1]}(\zeta,\xi)$. Further, if $S \subset \boldsymbol{\mu}_6$ is any set of roots of unity, we write $M_{\mathfrak{K}}(S)$ for the union of $M_{\mathfrak{K}}(\zeta)$ with $\zeta \in S$. With this notation, the four cases defining M_k are given by

(a) $M_k = M_k\big(\{\omega, \omega^5\}\big)$, (b) $M_k = M_k\big(\{\omega, \omega^3, \omega^5\}\big)$,

(c) $M_k = M_k\big(\{\omega, \omega^2, \omega^4, \omega^5\}\big)$, (d) $M_k = M_k(\boldsymbol{\mu}_6)$,

and in all cases, $M_k^{[1]} = M_k^{[1]}(S,1)$, where $S \subset \boldsymbol{\mu}_6$ is the set for the appropriate case.

We now restrict attention to the case that $k \in \mathbb{Z}$ is a rational prime with $\gcd(6,k) = 1$. If $k \equiv 2 \pmod 3$, so k is inert in K, then the computation of M_k and $M_k^{[1]}$ takes place in the field $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_{k^2}$ with k^2 elements. On the other hand, if $k \equiv 1 \pmod 3$, so k splits as $k\mathcal{O}_K = \mathfrak{K}\bar{\mathfrak{K}}$, then

$$\frac{\mathcal{O}_K}{k\mathcal{O}_K} \cong \frac{\mathcal{O}_K}{\mathfrak{K}} \times \frac{\mathcal{O}_K}{\bar{\mathfrak{K}}} \cong \mathbb{F}_k \times \mathbb{F}_k.$$

In this case a condition such as $\left(\frac{\lambda}{k}\right)_3 \neq 1$ becomes more complicated, since there are many ways for the product $\left(\frac{\lambda}{\mathfrak{K}}\right)_3\left(\frac{\lambda}{\mathfrak{K}}\right)_3$ to be different from 1.

Proposition 33. *Let $k \geq 5$ be a rational prime. The following table gives the values of $\#M_k(S)$ for various subsets $S \subset \boldsymbol{\mu}_6$, divided into cases according to whether k is split or inert in $K = \mathbb{Q}(\sqrt{-3}\,)$.*

		$k \equiv 1 \pmod 3$	$k \equiv 2 \pmod 3$
(a)	$\#M_k\big(\{\omega, \omega^5\}\big)$	$\frac{1}{3}(k-1)(k-3)$	$\frac{1}{3}(k^2-1)$
(b)	$\#M_k\big(\{\omega, \omega^3, \omega^5\}\big)$	$\frac{1}{2}(k-1)(k-3)$	$\frac{1}{2}(k^2-1)$
(c)	$\#M_k\big(\{\omega, \omega^2, \omega^4, \omega^5\}\big)$	$\frac{2}{3}(k-1)(k-3)$	$\frac{2}{3}(k^2-1)$
(d)	$\#M_k(\boldsymbol{\mu}_6)$	$(k-2)^2$	k^2-2

Proof. Suppose first that k is inert, so $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_{k^2}$. Then $\#M_k(\boldsymbol{\mu}_6)$ simply counts the $\lambda \in \mathbb{F}_{k^2}$ such that λ and $1-\lambda$ are units, so is equal to k^2-2. Next, $\#M_k\big(\{\omega, \omega^3, \omega^5\}\big)$ counts the quadratic non-residues in $\mathbb{F}_{k^2}$, of which there are $\frac{1}{2}(k^2-1)$. (Here the condition that $1-\lambda$ be a unit is irrelevant, since 1 is a quadratic residue). Similarly, $\#M_k\big(\{\omega, \omega^2, \omega^4, \omega^5\}\big)$ counts cubic non-residues in $\mathbb{F}_{k^2}$, of which there are $\frac{2}{3}(k^2-1)$. Finally, $\#M_k\big(\{\omega, \omega^5\}\big)$ counts the elements that are neither quadratic nor cubic residues, of which there are $\frac{1}{3}(k^2-1)$.

Next suppose that k splits, so $\mathcal{O}_K/k\mathcal{O}_K \cong \mathbb{F}_k \times \mathbb{F}_k$. Then $\#M_k(\boldsymbol{\mu}_6)$ counts $(a,b) \in \mathbb{F}_k^2$ with neither a nor b equal to 0 or 1. This gives $k-2$ possibilities for each of a and b, so $\#M_k(\boldsymbol{\mu}_6) = (k-2)^2$.

The required calculations for each of the remaining cases have much in common, so we will only illustrate the case of $M_k\big(\{\omega, \omega^3, \omega^5\}\big)$. Exactly $\frac{1}{2}$ of invertible (a,b) are quadratic non-residues. Therefore, there are $\frac{1}{2}(k-1)^2$ such elements. Of these, there are $\frac{1}{2}(k-1)$ of the form $(1,b)$ and $\frac{1}{2}(k-1)$ of the form $(a,1)$. The set $M_k\big(\{\omega, \omega^3, \omega^5\}\big)$ counts invertible (a,b) that are quadratic non-residues having $a \neq 1$ and $b \neq 1$. Therefore

$$\#M_k\big(\{\omega, \omega^3, \omega^5\}\big) = \frac{1}{2}(k-1)^2 - 2\left(\frac{1}{2}(k-1)\right) = \frac{1}{2}(k-1)(k-3).$$

(Note that $(1,1)$ is a quadratic residue, so the invertible non-residues of the form $(a,1)$ and $(1,b)$ are disjoint.) A similar argument applies to the two remaining cases, where we rely on the fact that invertible elements of $\mathbb{F}_k \times \mathbb{F}_k$ and of $\mathbb{F}_k$ fall evenly into the six sextic residue classes. $\square$

The table in Proposition 33 gives the value of $\#M_k(S)$ for the four subsets $S \subset \boldsymbol{\mu}_6$ that appear in Conjecture 30. It remains to construct a similar table for the values of $\#M_k^{[1]}(S)$. It turns out that these values can be expressed in terms of the number of points on a certain curve of genus four over various finite fields. We begin with a description of the curve that we need, after which we count points in order to compute the desired values.

Proposition 34. *Let $\mathbb{F}$ be a perfect field of characteristic not equal to 2 or 3. For $\kappa \in \mathbb{F}^*$ we define $E^{(\kappa)}$ to be the elliptic curve*

$$E^{(\kappa)} : y^2 = x^3 + \kappa,$$

and for $\gamma, \delta \in \mathbb{F}^*$ we define $C_6^{(\gamma,\delta)}$ to be a smooth projective model for the algebraic curve given by the affine equation

$$C_6^{(\gamma,\delta)} : \gamma z^6(1 - \gamma z^6) = \delta x^3.$$

(a) *The curve $C_6^{(\gamma,\delta)}$ has genus four.*

(b) *There are finite maps from $C_6^{(\gamma,\delta)}$ to curves of the form $E^{(\kappa)}$ given by the following formulas*:

$$\begin{aligned}
C_6^{(\gamma,\delta)} &\longrightarrow E^{(16\delta^2)}, && (x,z) \longmapsto (-4\delta x, 8\gamma\delta z^6 - 4\delta),\\
C_6^{(\gamma,\delta)} &\longrightarrow E^{(4\gamma^3\delta^4)}, && (x,z) \longmapsto \left(\frac{\delta^2 x^2}{z^6}, \gamma^2\delta^2 z^3 + \frac{\gamma\delta^2}{z^3}\right),\\
C_6^{(\gamma,\delta)} &\longrightarrow E^{(\gamma^5\delta^2)}, && (x,z) \longmapsto \left(\frac{\gamma\delta x}{z^4}, \frac{\gamma^2\delta}{z^3}\right),\\
C_6^{(\gamma,\delta)} &\longrightarrow E^{(-\gamma\delta^2)}, && (x,z) \longmapsto \left(-\frac{\delta x}{z^2}, \gamma\delta z^3\right).
\end{aligned}$$

(c) *The maps in* (b) *are independent, hence they induce an isogeny*

$$E^{(16\delta^2)} \times E^{(4\gamma^3\delta^4)} \times E^{(\gamma^5\delta^2)} \times E^{(-\gamma\delta^2)} \longrightarrow J_6^{(\gamma,\delta)} \stackrel{\text{def}}{=} \operatorname{Jac}(C_6^{(\gamma,\delta)}).$$

(d) *For any prime ℓ different from the characteristic of $\mathbb{F}$, we have isomorphisms of $\operatorname{Gal}(\bar{\mathbb{F}}/\mathbb{F})$-modules,*

$$\begin{aligned}
H^1_{\acute{e}t}\big(C^{(\gamma,\delta)}_{6/\mathbb{F}}, \mathbb{Q}_\ell\big) &\cong H^1_{\acute{e}t}\big(J^{(\gamma,\delta)}_{6/\mathbb{F}}, \mathbb{Q}_\ell\big)\\
&\cong H^1_{\acute{e}t}\big(E^{(16\delta^2)}_{/\mathbb{F}}, \mathbb{Q}_\ell\big) \times H^1_{\acute{e}t}\big(E^{(4\gamma^3\delta^4)}_{/\mathbb{F}}, \mathbb{Q}_\ell\big)\\
&\qquad \times H^1_{\acute{e}t}\big(E^{(\gamma^5\delta^2)}_{/\mathbb{F}}, \mathbb{Q}_\ell\big) \times H^1_{\acute{e}t}\big(E^{(-\gamma\delta^2)}_{/\mathbb{F}}, \mathbb{Q}_\ell\big).
\end{aligned}$$

Proof. (a) All of the $C_6^{(\gamma,\delta)}$ curves are geometrically isomorphic, so it suffices to calculate the genus of $C_6^{(1,1)}$, which for convenience we denote C_6. A simple calculation shows that the projective closure of C_6

in $\mathbb{P}^2$ is singular at $(0,0)$ and at the point at infinity, and that each of these singular points resolves to three points on the smooth model. (See Proposition 35 for details.) We let C_1 be the elliptic curve

$$C_1 : z(1-z) = x^3,$$

and we consider the natural degree 6 map

$$\psi : C_6 \longrightarrow C_1, \qquad (x,z) \longmapsto (x,z^6).$$

The map ψ is ramified only at $(0,0)$ and ∞, the sets $\psi^{-1}(0,0)$ and $\psi^{-1}(\infty)$ each consist of three points, and each of these points has ramification index 2. Applying the Riemann–Hurwitz genus formula to ψ gives

$$2g(C_6)-2 = 6\big(2g(C_1)-2\big) + \sum_{P\in C_1} \big(e_P(\psi)-1\big) = 6(2-2)+6(2-1) = 6.$$

Hence $g(C_6) = 4$.

(b) It is an exercise to verify that the given maps are well-defined, but we briefly comment on their origin. The automorphism group of the curve $C_6^{(\gamma,\delta)}$ is fairly large, since

$$\boldsymbol{\mu}_3 \times \boldsymbol{\mu}_6 \subset \mathrm{Aut}(C_6^{(\gamma,\delta)}), \qquad [\zeta,\xi](x,z) = (\zeta x, \xi z).$$

Taking quotients of $C_6^{(\gamma,\delta)}$ by various subgroups of $\boldsymbol{\mu}_3 \times \boldsymbol{\mu}_6$ gives maps to curves of lower genus, which in turn give the four maps described in (b).

(c) From general principles, the maps in (b) induce isogenies $E^{(\kappa)} \to J_6^{(\gamma,\delta)}$ for the given values of κ. There are various ways to see that these isogenies are independent. For example, one can use the fact that the four $E^{(\kappa)}$ are non-isogenous over $\mathbb{C}(\gamma,\delta)$, treating γ and δ as indeterminates. Or, at least in characteristic 0, one can take $\gamma = \delta = 1$, untwist to get four maps $C_6^{(1,1)} \to E^{(1)}$ defined over $\bar{\mathbb{Q}}$, and use the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the maps to show that they are independent. (See Appendix B.) Or, for a purely geometric proof, one can use intersection theory and the fact that the pairing

$$\langle\, \cdot\,,\, \cdot\,\rangle : \mathrm{Map}(C_6^{(1,1)}, E^{(1)})/E^{(1)} \to \mathbb{Z},$$
$$\langle \phi, \psi\rangle = \deg(\phi+\psi) - \deg\phi - \deg\psi,$$

is a positive definite quadratic form. (The $E^{(1)}$ in the denominator is shorthand for the right action of the group of translations.)

(d) It is a standard fact that $H^1_{\text{ét}}$ of a curve and its Jacobian are isomorphic. This gives the first isomorphism, and the second follows from (c) and the fact that an isogeny between abelian varieties induces an isomorphism of their étale cohomologies. □

Proposition 35. *Let $\mathfrak{K}$ be a prime ideal in $\mathcal{O}_K$ such that $\boldsymbol{\mu}_6 \subset \mathcal{O}_K/\mathfrak{K}$, i.e., $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{K}) \equiv 1 \pmod 6$. Let $\zeta \in \boldsymbol{\mu}_6$ and $\xi \in \boldsymbol{\mu}_3$, choose elements $\gamma, \delta \in \mathcal{O}_K$ satisfying $\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = \zeta$ and $\left(\frac{\delta}{\mathfrak{K}}\right)_3 = \xi$, and let $C_6^{(\delta,\gamma)}$ be the smooth projective curve from Proposition 34 given by the affine equation*

$$C_6^{(\gamma,\delta)} : \gamma z^6(1-\gamma z^6) = \delta x^3.$$

Then

$$\#M_{\mathfrak{K}}^{[1]}(\zeta,\xi) = \frac{1}{18}\left(\#C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) - e(\zeta,\xi)\right),$$

where the error term $e(\zeta,\xi)$ is given by the formula

$$e(\zeta,\xi) = \begin{bmatrix} 6 & \text{if } \zeta = 1 \\ 0 & \text{if } \zeta \ne 1 \end{bmatrix} + \begin{bmatrix} 3 & \text{if } \zeta^2 = \xi \\ 0 & \text{if } \zeta^2 \ne \xi \end{bmatrix} + \begin{bmatrix} 3 & \text{if } \zeta^4 = \xi \\ 0 & \text{if } \zeta^4 \ne \xi \end{bmatrix}.$$

Proof. Our choice of γ and δ imply that for any $\lambda \in \mathcal{O}_K$,

$$\begin{aligned} \left(\frac{\lambda}{\mathfrak{K}}\right)_6 = \zeta \quad &\Longleftrightarrow \quad \gamma^{-1}\lambda \equiv \text{non-zero sixth power } (\mathrm{mod}\ \mathfrak{K}), \\ \left(\frac{\lambda(1-\lambda)}{\mathfrak{K}}\right)_3 = \xi \quad &\Longleftrightarrow \quad \delta^{-1}\lambda(1-\lambda) \equiv \text{non-zero cube } (\mathrm{mod}\ \mathfrak{K}). \end{aligned}$$

We thus get a natural map

$$\begin{aligned} \left\{(x,z) \in C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) : x \ne 0, \infty\right\} &\longrightarrow M_{\mathfrak{K}}(\zeta,\xi), \\ (x,z) &\longmapsto \gamma z^6. \end{aligned} \tag{31}$$

We claim that the map (31) is exactly 18-to-1. To see this, let $\lambda \in M_{\mathfrak{K}}(\zeta,\xi)$. Then $\lambda \equiv \gamma v^6 \pmod{\mathfrak{K}}$ and $\lambda(1-\lambda) \equiv \delta u^3 \pmod{\mathfrak{K}}$ for some $u, v \in (\mathcal{O}_K/\mathfrak{K})^*$, so λ is the image of the point $(u,v) \in C_6^{(\gamma,\delta)}(\mathcal{O}_K/\mathfrak{K})$. Further, for a given value of λ, there are six choices for v and three choices for u. (Note that $\mathcal{O}_K/\mathfrak{K}$ contains $\boldsymbol{\mu}_6$.) Hence

$$\#M_{\mathfrak{K}}(\zeta,\xi) = \frac{1}{18}\#\left(C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) \smallsetminus \{x = 0 \text{ or } \infty\}\right).$$

It remains to count the number of $\mathcal{O}_K/\mathfrak{K}$-rational points with $x = 0$ or ∞ on a smooth model of $C_6^{(\gamma,\delta)}$.

To ease notation, we let $C = C_6^{(\gamma,\delta)}$, and we let C' be the curve

$$C' : \gamma(1-\gamma z^6) = \delta x^3. \tag{32}$$

The birational map

$$C \longrightarrow C', \qquad (x,z) \longmapsto (xz^{-2}, z),$$

is a bijection on the set of points

$$C \smallsetminus \{x = 0 \text{ or } \infty\} \quad \xleftrightarrow{\sim} \quad C' \smallsetminus \{x = 0 \text{ or } \infty\} \cup \{z = 0\},$$

and the affine piece of C' defined by equation (32) is smooth, so the points with $x = 0$ on C become the points with $x = 0$ or $z = 0$ on C'. (More precisely, we will see that the singular point $(0, 0) \in C$ is blown up to three points on C', while there are six smooth points of the form $(0, \gamma^{-1/6})$ on both C and C'.) The points on C' with $x = 0$ or $z = 0$ are characterized by

$$(0, z) \in C' \iff z^6 = \gamma^{-1} \qquad \text{and} \qquad (x, 0) \in C' \iff x^3 = \gamma\delta^{-1}.$$

Thus there are points of the form $(0, z)$ if and only if $\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = 1$, and there are points of the form $(0, x)$ if and only if $\left(\frac{\gamma\delta^{-1}}{\mathfrak{K}}\right)_3 = 1$. Using the values $\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = \zeta$ and $\left(\frac{\gamma\delta^{-1}}{\mathfrak{K}}\right)_3 = \left(\frac{\gamma}{\mathfrak{K}}\right)_6^2 \left(\frac{\delta^{-1}}{\mathfrak{K}}\right)_3 = \zeta^2\xi^{-1}$, we find that

$$\#\left\{(0, z) \in C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)\right\} = \begin{cases} 6 & \text{if } \zeta = 1, \\ 0 & \text{if } \zeta \neq 1, \end{cases}$$

$$\#\left\{(x, 0) \in C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)\right\} = \begin{cases} 3 & \text{if } \zeta^2 = \xi, \\ 0 & \text{if } \zeta^2 \neq \xi. \end{cases}$$

It remains to count the points at infinity on C'. Homogenizing the equation for C' gives the curve $\gamma y^6 - \gamma^2 z^6 = \delta x^3 y^3$. The unique (singular) point at infinity is $[x, y, z] = [1, 0, 0]$, so dehomogenizing by setting $x = 1$ gives the curve

$$\gamma y^6 - \gamma^2 z^6 = \delta y^3.$$

We blow up the singular point $(0, 0)$ by setting $y = z^2 u$. (This corresponds to blowing up twice. One can check that the other coordinate charts do not yield any additional points.) The resulting curve has affine equation

$$\gamma z^6 u^6 - \gamma^2 = \delta u^3.$$

This affine curve is smooth, and the points that map to the point at infinity on C' are the points with $z = 0$ and $u^3 = -\gamma^2\delta^{-1}$. Using $\left(\frac{\gamma^2\delta^{-1}}{\mathfrak{K}}\right)_3 = \left(\frac{\gamma}{\mathfrak{K}}\right)_6^4 \left(\frac{\delta^{-1}}{\mathfrak{K}}\right)_3$, we see that

$$\#\left\{\text{points at infinity on } C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right)\right\} = \begin{cases} 3 & \text{if } \zeta^4 = \xi, \\ 0 & \text{if } \zeta^4 \neq \xi. \end{cases}$$

This completes the proof of the proposition. □

The next step is to count the number of points on $C_6^{(\gamma,\delta)}$ defined over a finite field. This is done using the decomposition of $J_6^{(\gamma,\delta)}$ into a product of elliptic curves.

Proposition 36. *With notation as in the statement of Proposition 35, choose an element $\pi \in \mathcal{O}_K$ satisfying $\mathfrak{K} = \pi\mathcal{O}_K$ and $\pi \equiv 2 \pmod 3$. Further let $\epsilon = \left(\frac{2}{\mathfrak{K}}\right)_3$. Then*

$$\#C_6^{(\gamma,\delta)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) = \mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} + 1 + \mathrm{Tr}_{K/\mathbb{Q}}(\xi\bar{\pi}) + \mathrm{Tr}_{K/\mathbb{Q}}(\epsilon^2\zeta^3\xi^2\bar{\pi}) + \mathrm{Tr}_{K/\mathbb{Q}}(\epsilon\zeta^5\xi\bar{\pi}) + (-1)^{\frac{1}{2}(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K}-1)}\,\mathrm{Tr}_{K/\mathbb{Q}}(\epsilon\zeta\xi\bar{\pi}).$$

If $\mathfrak{K}$ is an inert prime, say $\mathfrak{K} = k\mathcal{O}_K$ with $k \in \mathbb{Z}$ satisfying $k \equiv 2 \pmod 3$, and if we take $\delta = 1$, then the formula simplifies to

$$\#C_6^{(\gamma,1)}\left(\frac{\mathcal{O}_K}{\mathfrak{K}}\right) = \begin{cases} k^2+1+8k & \text{if } \zeta = 1, \\ k^2+1-4k & \text{if } \zeta = -1, \\ k^2+1+2k & \text{if } \zeta \neq \pm 1. \end{cases}$$

Proof. To ease notation, let $\mathbb{F}_{\mathfrak{K}} = \mathcal{O}_K/\mathfrak{K}$, so $\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} = \#\mathbb{F}_{\mathfrak{K}}$. Further let $F_{\mathfrak{K}}$ be the $(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K})^{\text{th}}$-power Frobenius map on $\bar{\mathbb{F}}_{\mathfrak{K}}$. Then the number of points in $C_6^{(\gamma,\delta)}(\mathbb{F}_{\mathfrak{K}})$ is given by the trace formula [6, C.4.2],

$$\#C_6^{(\gamma,\delta)}(\mathbb{F}_{\mathfrak{K}}) = \mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} + 1 - \mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(C^{(\gamma,\delta)}_{6/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big). \tag{33}$$

We compute the trace using Proposition 34, which splits the representation for $C_6^{(\gamma,\delta)}$ into a product of representations on elliptic curves with zero j-invariant. Thus

$$\begin{aligned}\mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(C^{(\gamma,\delta)}_{6/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) &= \mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(E^{(16\delta^2)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) + \mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(E^{(4\gamma^3\delta^4)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) \\ &\quad + \mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(E^{(\gamma^5\delta^2)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) + \mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(E^{(-\gamma\delta^2)}_{/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big). \end{aligned} \tag{34}$$

We now apply [7, Chapter 18, Section 3, Theorem 4], which gives a formula for the trace in terms of residue symbols. Writing $\mathfrak{K} = \pi\mathcal{O}_K$ with $\pi \equiv 2 \pmod 3$, we find that

$$\begin{aligned}\mathrm{Tr}\Big(F_{\mathfrak{K}} \;\Big|\; H^1_{\text{ét}}(C^{(\gamma,\delta)}_{6/\mathbb{F}_{\mathfrak{K}}}, \mathbb{Q}_\ell)\Big) &= -\left(\frac{2^6\delta^2}{\mathfrak{K}}\right)_6^{-1}\pi - \left(\frac{2^6\delta^2}{\mathfrak{K}}\right)_6\bar{\pi} - \left(\frac{2^4\gamma^3\delta^4}{\mathfrak{K}}\right)_6^{-1}\pi - \left(\frac{2^4\gamma^3\delta^4}{\mathfrak{K}}\right)_6\bar{\pi} \\ &\quad - \left(\frac{2^2\gamma^5\delta^2}{\mathfrak{K}}\right)_6^{-1}\pi - \left(\frac{2^2\gamma^5\delta^2}{\mathfrak{K}}\right)_6\bar{\pi} - \left(\frac{-2^2\gamma\delta^2}{\mathfrak{K}}\right)_6^{-1}\pi - \left(\frac{-2^2\gamma\delta^2}{\mathfrak{K}}\right)_6\bar{\pi}\end{aligned}$$

$$= -\xi^{-1}\pi - \xi\bar{\pi} - \left(\frac{2}{\mathfrak{K}}\right)_3^{-2}\zeta^{-3}\xi^{-2}\pi - \left(\frac{2}{\mathfrak{K}}\right)_3^{2}\zeta^{3}\xi^{2}\bar{\pi}$$
$$- \left(\frac{2}{\mathfrak{K}}\right)_3^{-1}\zeta^{-5}\xi^{-1}\pi - \left(\frac{2}{\mathfrak{K}}\right)_3\zeta^{5}\xi\bar{\pi}$$
$$- \left(\frac{-1}{\mathfrak{K}}\right)_2\left(\frac{2}{\mathfrak{K}}\right)_3^{-1}\zeta^{-1}\xi^{-1}\pi - \left(\frac{-1}{\mathfrak{K}}\right)_2\left(\frac{2}{\mathfrak{K}}\right)_3\zeta\xi\bar{\pi}. \tag{35}$$

Noting that $\left(\frac{-1}{\mathfrak{K}}\right)_2 = (-1)^{(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K}-1)/2}$, we combine (33) and (35) to obtain the desired result.

In the case that $\mathfrak{K} = k\mathcal{O}_K$ is an inert prime, we have $(-1)^{\frac{1}{2}(k^2-1)} = 1$ since k is odd. Further, both 2 and k are primary, so cubic reciprocity gives $\left(\frac{2}{\mathfrak{K}}\right)_3 = \left(\frac{2}{k}\right)_3 = \left(\frac{k}{2}\right)_3 = 1$. Further taking $\delta = 1$ implies that $\xi = 1$, so the formula for $\#C_6^{(\gamma,1)}(\mathcal{O}_K/\mathfrak{K})$ becomes

$$k^2 + 1 + \big(\mathrm{Tr}_{K/\mathbb{Q}}(1) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta^3) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta^5) + \mathrm{Tr}_{K/\mathbb{Q}}(\zeta)\big)k.$$

Taking the six possible values $\zeta \in \boldsymbol{\mu}_6$ yields the stated formula. □

Proposition 37. *Let $k \geq 5$ be a rational prime. The following table gives the values of $\#M_k^{[1]}(S,1)$ for various subsets $S \subset \boldsymbol{\mu}_6$, divided into cases according to whether k is split or inert in $K = \mathbb{Q}(\sqrt{-3}\,)$, cf. Proposition 33.*

		$k \equiv 1 \pmod 3$	$k \equiv 2 \pmod 3$
(a)	$\#M_k^{[1]}\big(\{\omega,\omega^5\},1\big)$	$\frac{1}{9}(k-1)^2$	$\frac{1}{9}(k+1)^2$
(b)	$\#M_k^{[1]}\big(\{\omega,\omega^3,\omega^5\},1\big)$	$\frac{1}{6}(k-1)(k-3)$	$\frac{1}{6}(k^2-1)$
(c)	$\#M_k^{[1]}\big(\{\omega,\omega^2,\omega^4,\omega^5\},1\big)$	$\frac{2}{9}(k-1)^2$	$\frac{2}{9}(k+1)^2$
(d)	$\#M_k^{[1]}(\boldsymbol{\mu}_6,1)$	$\frac{1}{3}(k^2-2k+4)$	$\frac{1}{3}(k^2+2k-2)$

Proof. We begin with the case that $k \equiv 2 \pmod 3$, so $\mathfrak{K} = k\mathcal{O}_K$ is a prime ideal with $\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{K} = k^2$. We let $\omega = \frac{1}{2}(1+\sqrt{-3})$ be the usual sixth root of unity, and we choose some $\gamma \in \mathcal{O}_K$ satisfying

$$\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = \omega.$$

Then for any $0 \leq i \leq 5$ we have

$$18\#M_k^{[1]}(\omega^i,1) = \#C_6^{(\gamma^i,1)}(\mathbb{F}_{\mathfrak{K}}) - \begin{bmatrix} 12 & \text{if } i = 0 \\ 6 & \text{if } i = 3 \\ 0 & \text{otherwise} \end{bmatrix}$$

from Proposition 35 with $\zeta = \omega^i$ and $\xi = 1$,

$$= \begin{bmatrix} k^2+1+8k & \text{if } i=0 \\ k^2+1-4k & \text{if } i=3 \\ k^2+1+2k & \text{otherwise} \end{bmatrix} - \begin{bmatrix} 12 & \text{if } i=0 \\ 6 & \text{if } i=3 \\ 0 & \text{otherwise} \end{bmatrix}$$

from Proposition 36 with $\zeta = \omega^i$ and $\xi = 1$,

$$= \begin{cases} k^2+8k-11 & \text{if } i=0, \\ k^2-4k-5 & \text{if } i=3, \\ k^2+2k+1 & \text{otherwise.} \end{cases}$$

It is now easy to compute $\#M_k^{[1]}(S,1) = \sum_{\zeta\in S} \#M_k^{[1]}(\zeta,1)$ for the four cases of the proposition. For example,

$$\begin{aligned} \#M_k^{[1]}(\boldsymbol{\mu}_6,1) &= \frac{1}{18}\big((k^2+8k-11)+(k^2-4k-5)+4(k^2+2k+1)\big) \\ &= \frac{1}{3}(k^2+2k-2). \end{aligned}$$

Next we consider the case that $k \equiv 1 \pmod 3$, so $k\mathcal{O}_K = \mathfrak{K}\bar{\mathfrak{K}}$ splits. The definition of the residue symbol says that

$$\left(\frac{\lambda}{k\mathcal{O}_K}\right)_6 = \left(\frac{\lambda}{\mathfrak{K}}\right)_6 \left(\frac{\lambda}{\bar{\mathfrak{K}}}\right)_6,$$
$$\left(\frac{\lambda(1-\lambda)}{k\mathcal{O}_K}\right)_3 = \left(\frac{\lambda(1-\lambda)}{\mathfrak{K}}\right)_3 \left(\frac{\lambda(1-\lambda)}{\bar{\mathfrak{K}}}\right)_3,$$

so using the Chinese remainder theorem

$$\mathcal{O}_K/k\mathcal{O}_K = \mathcal{O}_K/\mathfrak{K}\mathcal{O}_K \times \mathcal{O}_K/\bar{\mathfrak{K}}\mathcal{O}_K,$$

a quantity such as $M_k^{[1]}(\zeta,\xi)$ breaks up into a sum of products,

$$M_k^{[1]}(\zeta,\xi) = \sum_{u=0}^{5}\sum_{v=0}^{2} M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v}) M_{\bar{\mathfrak{K}}}^{[1]}(\zeta\omega^{-u},\xi\omega^{-2v}).$$

Hence for $0 \le i \le 5$ we have

$$\begin{aligned} M_k^{[1]}(\omega^i,1) &= \sum_{u=0}^{5}\sum_{v=0}^{2} M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v}) M_{\bar{\mathfrak{K}}}^{[1]}(\omega^{i-u},\omega^{-2v}) \\ &= \sum_{u=0}^{5}\sum_{v=0}^{2} M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v}) M_{\mathfrak{K}}^{[1]}(\omega^{u-i},\omega^{2v}). \end{aligned} \tag{36}$$

(For the second equality we've used the identity $M_{\mathfrak{K}}^{[1]}(\zeta,\xi) = M_{\bar{\mathfrak{K}}}^{[1]}(\bar{\zeta},\bar{\xi})$.) We choose γ and δ to satisfy

$$\left(\frac{\gamma}{\mathfrak{K}}\right)_6 = \omega \qquad \text{and} \qquad \left(\frac{\delta}{\mathfrak{K}}\right)_3 = \omega^2.$$

Then Proposition 35 gives us the formula

$$18M_{\mathfrak{K}}^{[1]}(\omega^u,\omega^{2v}) = \#C_6^{(\gamma^u,\delta^v)}(\mathbb{F}_{\mathfrak{K}}) - e(\omega^u,\omega^{2v}), \tag{37}$$

where

$$e(\omega^u,\omega^{2v}) = \begin{bmatrix} 6 & \text{if } u \equiv 0 \pmod 6 \\ 0 & \text{otherwise} \end{bmatrix} + \begin{bmatrix} 3 & \text{if } u \equiv v \pmod 3 \\ 0 & \text{otherwise} \end{bmatrix} + \begin{bmatrix} 3 & \text{if } 2u \equiv v \pmod 3 \\ 0 & \text{otherwise} \end{bmatrix}. \tag{38}$$

Further, Proposition 36 gives us the number of points on the curve,

$$\begin{aligned} \#C_6^{(\gamma^u,\delta^v)}(\mathbb{F}_{\mathfrak{K}}) &= k+1+\operatorname{Tr}_{K/\mathbb{Q}}(\omega^{2v}\bar{\pi}) + \operatorname{Tr}_{K/\mathbb{Q}}(\epsilon^2\omega^{3u+4v}\bar{\pi}) \\ &\quad + \operatorname{Tr}_{K/\mathbb{Q}}(\epsilon\omega^{5u+2v}\bar{\pi}) + (-1)^{\frac{1}{2}(k-1)}\operatorname{Tr}_{K/\mathbb{Q}}(\epsilon\omega^{u+2v}\bar{\pi}), \end{aligned} \tag{39}$$

where $\epsilon = \left(\frac{2}{\mathfrak{K}}\right)_3$.

Combining (36), (37), (38), and (39) gives an explicit, albeit quite complicated, formula for $M_k^{[1]}(\omega^i,1)$. In principle, this formula could be computed by hand, but we are content to evaluate it using PARI [26], which yields the following values:

$$18\#M_k^{[1]}(\omega^i,1) = \begin{cases} k^2+4k+13 & \text{if } i=0, \\ k^2-8k+7 & \text{if } i=3, \\ k^2-2k+1 & \text{otherwise.} \end{cases}$$

(See Remark 38 for further information about this computation.) It is now a simple matter to compute the value of $\#M_k^{[1]}(S,1)$ for the four cases. For example,

$$\begin{aligned} \#M_k^{[1]}(\boldsymbol{\mu}_6,1) &= \frac{1}{18}\big((k^2+4k+13)+(k^2-8k+7)+4(k^2-2k+1)\big) \\ &= \frac{1}{3}(k^2-2k+4). \end{aligned}$$

This completes the proof of Proposition 37. □

Remark 38. We used PARI [26] to compute $M_k^{[1]}(\omega^i,1)$ by evaluating formulas (36), (37), (38), and (39), where we treated k, π, and ϵ as indeterminates, and we formally set $\bar{\pi} = k/\pi$ and $\bar{\epsilon} = 1/\epsilon$. (The PARI code used for the computation is given in Appendix C.) The value of $M_k^{[1]}(\omega^i,1)$ turns out to be a quadratic polynomial in k that is independent of $k \bmod 4$. We do not have an *a priori* explanation for why this should be the case. In order to illustrate the delicacy of the

argument, we suppose for a moment that the isogeny decomposition of the Jacobian of $C_6^{(\gamma,\delta)}$ in Proposition 34 looks like

$$E^{(16\delta^2)} \times E^{(4\gamma^4\delta^4)} \times E^{(\gamma^5\delta^2)} \times E^{(-\gamma\delta^2)} \longrightarrow \mathrm{Jac}(C_6^{(\gamma,\delta)}).$$

(All that we have done is change the second elliptic factor from $E^{(4\gamma^3\delta^4)}$ to $E^{(4\delta^4)}$.) This would have the effect in formula (39) of changing the second trace term from $\mathrm{Tr}_{K/\mathbb{Q}}(\epsilon^2\omega^{3u+4v}\bar{\pi})$ to $\mathrm{Tr}_{K/\mathbb{Q}}(\epsilon^2\omega^{4v}\bar{\pi})$. But with this small modification, there is less cancelation in the computation of $M_k^{[1]}(\omega^i, 1)$, so for example $\#M_k^{[1]}\big(\{\omega, \omega^5\}, 1\big)$ would equal

$$\frac{1}{9}\left(k^2 + 2k + 1 + 2\,\mathrm{Tr}\left(\left(\frac{2}{\mathfrak{K}}\right)_3^2 \bar{\pi}^2\right)\right).$$

Thus $\#M_k^{[1]}\big(\{\omega, \omega^5\}, 1\big)$ would depend on both $\left(\frac{2}{\mathfrak{K}}\right)_3$ and on the factorization of k in $\mathcal{O}_K$.

Remark 39. Many of the cases of Proposition 37 can be obtained somewhat more easily by working on elliptic curves $z(1-z) = \delta x^3$ or genus two curves $\gamma z^2(1-\gamma z^2) = \delta x^3$. However, some cases require the curves $\gamma z^6(1-\gamma z^6) = \delta x^3$ of genus four, so for unity of exposition and to save space, we have derived all cases using these latter curves.

Combining Conjecture 30 with the computations in Propositions 33 and 37 yields precise formulas for the conjectural density of Type 1 primes on $y^2 = x^3 + k$ when k is prime.

Conjecture 40. *Let $k \geq 5$ be a rational prime. Then*

$$\lim_{X\to\infty} \frac{\mathcal{N}_k^{[1]}(X)}{\mathcal{N}_k(X)} = \frac{1}{3} + R(k),$$

where $R(k)$ depends on k (mod 36) *and is given by the following table*:

	k mod 36	$R(k)$
(a,c)	1, 19	$\dfrac{2}{3(k-3)}$
(b)	13, 25	0
(d)	7, 31	$\dfrac{2k}{3(k-2)^2}$

	k mod 36	$R(k)$
(a,c)	17, 35	$\dfrac{2}{3(k-1)}$
(b)	5, 29	0
(d)	11, 23	$\dfrac{2k}{3(k^2-2)}$

In particular, $R(k) = O(1/k)$.

We do not have an intrinsic explanation for why $R(k)$ is the same in cases (a) and (c), nor do we know why $R(k) = 0$ in case (b).

7. Amicable pairs for elliptic curves — Experiments

In this section we present the results of experiments that test the reasonableness of our conjectures. We begin with Conjecture 3, which deals with the case of CM curves having nonzero j-invariant.

We computed the number $\mathcal{Q}_E(X)$ of amicable pairs up to X for elliptic curves with CM by the imaginary quadratic order of discriminant $-D$ and conductor f. Theorem 13 says that it suffices to consider $D \equiv 3 \pmod 4$. Further, the assumption that E is defined over $\mathbb{Q}$ means that $\mathcal{O}$ has class number one, so the classification of imaginary quadratic fields of class number one combined with an elementary formula for the class number of an order [18, Exercise 4.12] imply that the only possibilities for D are $D \in \{3, 7, 11, 19, 43, 67, 163\}$, and the possible values of f are given by $f \in \{1, 2, 3\}$ if $D = 3$, $f \in \{1, 2\}$ if $D = 7$, and $f = 1$ in all other cases. See [19, A §3] for a Weierstrass equations for each CM type.

We ignore for the moment the case $(D, f) = (3, 1)$. As noted in the proof of Theorem 13, the curves with (D, f) equal to $(3, 2)$, $(7, 1)$, and $(7, 2)$ have nontrivial 2-torsion, so neither they nor any of their (necessarily quadratic) twists have amicable pairs. The curve with $(D, f) = (3, 3)$ listed in [19, A §3] has nontrivial 3-torsion, but it has quadratic twists with trivial torsion, so is a candidate to have amicable pairs. Table 2 lists the number $\mathcal{Q}_E(X)$ of amicable pairs up to the given bound and the ratio of $\mathcal{Q}_E(X)$ to the number $\mathcal{N}_E(X)$ of primes p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is prime. For this table we used the following Weierstrass equations.[1]

$$
\begin{aligned}
(D, f) = (3, 3) \qquad & y^2 = x^3 - 120x + 506, \\
(D, f) = (11, 1) \qquad & y^2 + y = x^3 - x^2 - 7x + 10, \\
(D, f) = (19, 1) \qquad & y^2 + y = x^3 - 38x + 90, \\
(D, f) = (43, 1) \qquad & y^2 + y = x^3 - 860x + 9707, \\
(D, f) = (67, 1) \qquad & y^2 + y = x^3 - 7370x + 243528, \\
(D, f) = (163, 1) \qquad & y^2 + y = x^3 - 2174420x + 1234136692.
\end{aligned}
$$

The results in Table 2 are consistant with Conjecture 18, which predicts that the ratio $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ should approach $\frac{1}{4}$.

[1] Calculations on quadratic twists of the listed curves yielded virtually identical results.

(D, f)	(3,3)	(11,1)	(19,1)	(43,1)	(67,1)	(163,1)
$\mathcal{Q}_E(10^5)$	124	48	103	205	245	395
$\mathcal{Q}_E(10^5)/\mathcal{N}_E(10^5)$	0.251	0.238	0.248	0.260	0.238	0.246
$\mathcal{Q}_E(10^6)$	804	303	709	1330	1671	2709
$\mathcal{Q}_E(10^6)/\mathcal{N}_E(10^6)$	0.250	0.247	0.253	0.255	0.245	0.247
$\mathcal{Q}_E(10^7)$	5581	2267	5026	9353	12190	19691
$\mathcal{Q}_E(10^7)/\mathcal{N}_E(10^7)$	0.249	0.251	0.250	0.251	0.250	0.252

TABLE 2. $\mathcal{Q}_E(X)$ and $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for elliptic curves with CM by $\mathbb{Q}(\sqrt{-D})$

k	2	3	5	6	7	10
$X = 10^5$	0.251	0.122	0.081	0.134	0.139	0.125
$X = 10^6$	0.250	0.139	0.083	0.142	0.133	0.107
$X = 10^7$	0.249	0.139	0.082	0.139	0.129	0.107

TABLE 3. $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ for elliptic curves $y^2 = x^3 + k$

We next considered the curves $y^2 = x^3 + k$ with $j(E) = 0$. Table 3, which is included for historical reasons, was our first intimation that the limiting value of $\mathcal{Q}_E(X)/\mathcal{N}_E(X)$ behaves differently for different values of k, with no obvious pattern for $2 \le k \le 10$. (Note that we do not list values of k that are squares or cubes, since in those cases $E(\mathbb{Q})_{\text{tors}}$ is nontrivial, so there are no amicable pairs.)

We recall the notation $\mathcal{N}_k^{[1]}$ for the set of Type 1 primes for the curve $y^2 = x^3 + k$; see Section 6 for the precise definition. Conjecture 27 predicts that $\mathcal{Q}_k(X) \sim \frac{1}{4}\mathcal{N}_k^{[1]}(X)$, and in the case that k is prime, Conjecture 40 says that

$$\mathcal{N}_k^{[1]}(X) \sim \left(\frac{1}{3} + R(k)\right)\mathcal{N}_k(X),$$

where $R(k)$ is given by an explicit formula that depends on k modulo 36. We tested these two conjectures by computing $\mathcal{Q}_k(X)$, $\mathcal{N}_k^{[1]}(X)$, and $\mathcal{N}_k(X)$ for $X = 10^8$. The results are listed in Table 4. Column 5 provides convincing evidence for Conjecture 27, and the final

two columns show that Conjecture 40 is in good agreement with experiment in all eight cases. (The notation $(x.n)$ after each value of k indicates the case $x = (a),\ldots,(d)$ and the congruence class $k \equiv n \pmod 3$ from Conjecture 40.)

					Density of Type 1 primes $\mathcal{N}_k^{[1]}(X)/\mathcal{N}_k(X)$	
k	$\mathcal{Q}_k(X)$	$\mathcal{N}_k^{[1]}(X)$	$\mathcal{N}_k(X)$	$\mathcal{Q}/\mathcal{N}^{[1]}$	experiment	conjecture
5 (b.2)	29340	58594	175703	0.251	0.3335	$\frac{1}{3} = 0.3333$
7 (d.1)	43992	87825	168743	0.251	0.5205	$\frac{13}{25} = 0.5200$
11 (d.2)	33721	66698	169062	0.253	0.3945	$\frac{47}{119} = 0.3950$
13 (b.1)	28036	55766	167333	0.252	0.3333	$\frac{1}{3} = 0.3333$
17 (a.2)	32008	63810	169226	0.251	0.3771	$\frac{3}{8} = 0.3750$
19 (c.1)	31729	63066	168196	0.252	0.3750	$\frac{3}{8} = 0.3750$
23 (d.2)	30480	61210	168512	0.249	0.3632	$\frac{191}{527} = 0.3624$
29 (b.2)	28085	56286	168642	0.249	0.3338	$\frac{1}{3} = 0.3333$
31 (d.1)	30301	60349	168344	0.251	0.3585	$\frac{301}{841} = 0.3579$
37 (a.1)	29728	59430	168471	0.250	0.3528	$\frac{6}{17} = 0.3529$
41 (b.2)	28050	56381	168567	0.249	0.3345	$\frac{1}{3} = 0.3333$
43 (d.1)	29619	58807	168410	0.252	0.3492	$\frac{589}{1681} = 0.3504$
47 (d.2)	29220	58400	168365	0.250	0.3469	$\frac{767}{2207} = 0.3475$
53 (a.2)	29278	58257	168353	0.252	0.3460	$\frac{9}{26} = 0.3462$
59 (d.2)	29378	58422	168783	0.252	0.3461	$\frac{1199}{3479} = 0.3446$
61 (b.1)	28027	55816	168197	0.251	0.3318	$\frac{1}{3} = 0.3333$
67 (d.1)	29242	57944	168239	0.253	0.3444	$\frac{1453}{4225} = 0.3439$
71 (c.2)	28789	57661	168508	0.249	0.3422	$\frac{12}{35} = 0.3429$
73 (a.1)	28975	57828	168614	0.251	0.3430	$\frac{12}{35} = 0.3429$
79 (d.1)	29127	57937	168690	0.252	0.3435	$\frac{2029}{5929} = 0.3422$
83 (d.2)	29032	57871	168435	0.251	0.3436	$\frac{2351}{6887} = 0.3414$
89 (a.2)	28909	57634	168737	0.251	0.3416	$\frac{15}{44} = 0.3409$
97 (b.1)	28014	55880	168457	0.251	0.3317	$\frac{1}{3} = 0.3333$

TABLE 4. Density of Amicable and Type 1 primes with $p \le X = 10^8$ for the curve $y^2 = x^3 + k$, prime k.

We also checked Conjecture 30 experimentally for composite values of k. The results are listed in Table 5, where the conjectural limiting ratio is obtained by explicitly counting the size of the sets $\mathcal{M}_k$ and $\mathcal{M}_k^{[1]}$. The top eight k entries in this table are products of two primes covering the usual eight cases; the final four entries include two values that are not square-free ($175 = 5 \cdot 7^2$ and $245 = 5 \cdot 7^2$) and two values that are products of three distinct primes ($385 = 5 \cdot 7 \cdot 11$ and $455 = 5 \cdot 7 \cdot 13$).

In order to further test the validity of Conjecture 30 , we recomputed the final entry in the table with $X = 10^9$ and obtained

$$\mathcal{N}_{455}^{[1]}(10^9)/\mathcal{N}_{455}(10^9) = 0.3380.$$

This is in excellent agreement with the theoretical value of $\frac{4699}{13915} = 0.3377$.

					Density of Type 1 primes $\mathcal{N}_k^{[1]}(X)/\mathcal{N}_k(X)$	
k	$\mathcal{Q}_k(X)$	$\mathcal{N}_k^{[1]}(X)$	$\mathcal{N}_k(X)$	$\mathcal{Q}/\mathcal{N}^{[1]}$	experiment	conjecture
35 (d.2)	31423	63169	168666	0.248	0.3745	$\frac{43}{115} = 0.3739$
55 (d.1)	29645	58718	168870	0.253	0.3477	$\frac{949}{2737} = 0.3467$
77 (b.2)	28170	56251	168921	0.251	0.3330	$\frac{1}{3} = 0.3333$
85 (b.1)	28187	56142	168767	0.251	0.3327	$\frac{1}{3} = 0.3333$
323 (c.2)	28396	56609	168585	0.251	0.3358	$\frac{43}{128} = 0.3359$
629 (a.2)	28210	56269	168042	0.251	0.3349	$\frac{3267}{9766} = 0.3345$
703 (c.1)	28558	56754	168817	0.252	0.3362	$\frac{1097}{3278} = 0.3347$
901 (a.1)	28341	56384	168411	0.252	0.3348	$\frac{3738}{11189} = 0.3341$
175 (d.1)	31543	63177	168840	0.250	0.3742	$\frac{43}{115} = 0.3739$
245 (b.2)	29722	58848	175934	0.253	0.3345	$\frac{1}{3} = 0.3333$
385 (b.1)	28070	56158	168393	0.250	0.3335	$\frac{1}{3} = 0.3333$
455 (d.2)	28346	56627	168342	0.250	0.3364	$\frac{4699}{13915} = 0.3377$

TABLE 5. Density of Amicable and Type 1 primes with $p \le X = 10^8$ for the curve $y^2 = x^3 + k$, composite k.

Finally, we consider Conjecture 9, which deals with non-CM curves. This conjecture is much harder to check numerically because the function $\sqrt{X}/(\log X)^2$ grows quite slowly. We performed an extended search for amicable pairs on the elliptic curve

$$E : y^2 + y = x^3 + x^2 \tag{40}$$

of conductor 43 that we studied in Example 1. Appendix D lists all normalized amicable pairs (p, q) with $p < 10^{11}$. Conjectures 3(a) and 9 says that $\mathcal{Q}_E(X)$, the number of amicable pairs up to X, should grow like a multiple of $\sqrt{X}/(\log X)^2$. Table 6 tests this conjecture by computing the ratios

$$\frac{\mathcal{Q}_E(X)}{\sqrt{X}/2(\log X)^2} \qquad \text{and} \qquad \frac{\log \mathcal{Q}_E(X)}{\log X}$$

for various values of X. The computations for Table 6, i.e., the computation of $\mathcal{Q}_E(10^{11})$, took approximately five days running in parallel on a cluster of ten machines. The third column of Table 6 provides some

small support for the conjecture that $\mathcal{Q}(X)$ grows like a multiple of $\sqrt{X}/(\log X)^2$. On the other hand, although the fourth column of the table suggests that $\mathcal{Q}(X)$ grows like X^δ for some $\delta > 0$, it is far from clear that δ is as large as $\frac{1}{2}$. We suspect the problem is that we are only able to compute $\mathcal{Q}(X)$ up to $X = 10^{11}$, and although 10^{11} is a moderately large number in terms of computation time, it is comparatively small compared to the likely error terms in any putative asymptotic formula for $\mathcal{Q}(X)$.

X	$\mathcal{Q}(X)$	$\mathcal{Q}(X)/\frac{\sqrt{X}}{(\log X)^2}$	$\frac{\log \mathcal{Q}(X)}{\log X}$
10^6	2	0.382	0.050
10^7	4	0.329	0.086
10^8	5	0.170	0.087
10^9	10	0.136	0.111
10^{10}	21	0.111	0.132
$2 \cdot 10^{10}$	32	0.127	0.146
$4 \cdot 10^{10}$	37	0.110	0.148
$6 \cdot 10^{10}$	44	0.111	0.152
$8 \cdot 10^{10}$	53	0.118	0.158
10^{11}	55	0.112	0.158

TABLE 6. Counting amicable pairs for $y^2 + y = x^3 + x^2$

Finally, we searched for normalized aliquot triples (p, q, r) on the curve (40). We found no examples with $p < 10^8$. To compare this to Conjecture 9, we consider the counting functions

$$\mathcal{P}_E^{[\ell]}(X) = \#\left\{(p_1, \dots, p_\ell) : \begin{array}{l} p_i \text{ distinct primes with } p_1 \le X \text{ and} \\ \#\tilde{E}_{p_i}(\mathbb{F}_{p_i}) = p_{i+1} \text{ for } 1 \le i \le \ell - 1 \end{array}\right\}.$$

Note that $\mathcal{P}_E^{[\ell]}(X)$ is not counting aliquot cycles, because we do not require that $\#\tilde{E}_{p_\ell}(\mathbb{F}_{p_\ell})$ equal p_1. A natural generalization of the Koblitz–Zywina conjecture (Conjecture 6) is that

$$\mathcal{P}_E^{[\ell]}(X) \sim C_{E/\mathbb{Q}}^{[\ell]} \frac{X}{(\log X)^\ell}.$$

We computed $\mathcal{P}_E^{[2]}(X)$ and $\mathcal{P}_E^{[3]}(X)$ for the curve (40) and used it to estimate the values of the constants $C_{E/\mathbb{Q}}^{[2]}$ and $C_{E/\mathbb{Q}}^{[3]}$. The results are listed in Table 7.

X	$\mathcal{P}_E^{[2]}(X)$	$\mathcal{P}_E^{[3]}(X)$	$C_{E/\mathbb{Q}}^{[2]}$	$C_{E/\mathbb{Q}}^{[3]}$	$\frac{1}{2}\mathcal{P}_E^{[3]}(X)X^{-1/2}$
10^5	485	21	0.643	0.320	0.033
10^6	3099	116	0.592	0.306	0.058
10^7	22328	741	0.580	0.310	0.117
10^8	168611	4995	0.572	0.312	0.250

TABLE 7. An aliquot triple estimate for $y^2 + y = x^3 + x^2$

Our heuristic argument from Section 3 suggests that if (p, q, r) is a triple counted in $\mathcal{P}_E^{[3]}(X)$, then the probability that $\#\tilde{E}_r(\mathbb{F}_r)$ equals p is $O(r^{-1/2})$, and more precisely, we expect it to be between $\frac{1}{2}r^{-1/2}$ and $\frac{1}{4}r^{-1/2}$. Thus the number of aliquot triples less than X should roughly be somewhere between

$$\frac{1}{2}\mathcal{P}_E^{[3]}(X)X^{-1/2} \qquad \text{and} \qquad \frac{1}{4}\mathcal{P}_E^{[3]}(X)X^{-1/2}. \tag{41}$$

The last column of Table 7 gives our heuristic upper bound for the number of aliquot triples up to X. It is thus not surprising that we found no examples up to 10^8. Using the estimate $C_{E/\mathbb{Q}}^{[3]} \approx 0.312$, setting $\mathcal{P}_E^{[3]}(X) \approx C_{E/\mathbb{Q}}^{[3]} \frac{X}{(\log X)^3}$, and taking the upper bound in (41), it would require at least $X \approx 5 \cdot 10^9$ in order to expect find an aliquot triple. And even for $X = 10^{11}$ we wouldn't expect more than two or three.

8. Motivation and generalizations

Remark 41. Elliptic amicable pairs and aliquot cycles appeared in a natural fashion when the authors were generalizing to elliptic divisibility sequences Smyth's results [23] on index divisibility of Lucas sequences. Let $(W_n)_{n\geq 1}$ be a normalized nonsingular nonperiodic elliptic divisibility sequence associated to an elliptic curve $E/\mathbb{Q}$, and consider the set

$$\mathcal{S} = \{n \geq 1 : n \mid W_n\}.$$

An element of $\mathcal{S}$ is called *basic* if $n/p \notin \mathcal{S}$ for all primes$p$ dividing n. It turns out that basic elements can be created using aliquot cycles, a phenomenon that does not occur in Smyth's work. More precisely, given any aliquot cycle $(p_1, \ldots, p_\ell)$ for $E/\mathbb{Q}$ of length $\ell \geq 2$, the product $p_1 p_2 \cdots p_\ell$ is a basic element for (W_n), and more generally, any product of such products is basic. See [21] for details.

Remark 42. As we have defined them, aliquot cycles for elliptic curves differ in a significant way from classical aliquot cycles associated to the sum of divisors function. In the classical case, every integer n leads to

a possibly non-repeating aliquot sequence $\big(n, \tilde{\sigma}(n), \tilde{\sigma}^2(n), \tilde{\sigma}^3(n), \ldots\big)$, and it is an aliquot cycle if some iterate $\tilde{\sigma}^k(n)$ eventually returns to n. (A major open problem is whether there are starting values for which the sequence is unbounded.) But for elliptic curves, if we arrive at a prime p such that $\#\tilde{E}_p(\mathbb{F}_p)$ is not prime, then the sequence cannot be continued. We propose here two alternative definitions of elliptic aliquot sequences that more closely resemble the classical definition. We leave the investigation of these generalized sequences to a future paper.

Definition. Let $E/\mathbb{Q}$ be an elliptic curve, let $L(E/\mathbb{Q}, s) = \sum_{n\ge 1} a_n/n^s$ be the L-series of E, and define a function

$$F_E : \mathbb{N} \longrightarrow \mathbb{N}, \qquad F_E(n) = n + 1 - a_n.$$

A *Type L aliquot sequence* for $E/\mathbb{Q}$ is a sequence obtained by starting at some $n \in \mathbb{N}$ and repeatedly applying the map F_E. A *Type L aliquot cycle* is a Type L aliquot sequence that repeats at its starting value.

Definition. Let $E/\mathbb{Q}$ be an elliptic curve, let $\mathcal{E}^0/\mathbb{Z}$ be the open subset of the Néron model for $E/\mathbb{Q}$ consisting of the connected components of each fiber, and define a function

$$G_E : \mathbb{N} \longrightarrow \mathbb{N}, \qquad G_E(n) = \#\mathcal{E}^0(\mathbb{Z}/n\mathbb{Z}).$$

A *Type N aliquot sequence* for $E/\mathbb{Q}$ is a sequence obtained by starting at some $n \in \mathbb{N}$ and repeatedly applying the map G_E. A *Type N aliquot cycle* is a Type N aliquot sequence that repeats at its starting value.

Remark 43. There is a natural way to generalize the notion of elliptic amicable pairs and aliquot cycles to elliptic curves defined over number fields. Thus let $F/\mathbb{Q}$ be a number field and E/F an elliptic curve. We will say that a sequence of distinct degree one prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_\ell$ is an *aliquot cycle* of length ℓ for E/F if E has good reduction at every $\mathfrak{p}_i$ and

$$\#\tilde{E}_{\mathfrak{p}_1}(\mathbb{F}_{\mathfrak{p}_1}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_2), \quad \#\tilde{E}_{\mathfrak{p}_2}(\mathbb{F}_{\mathfrak{p}_2}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_3), \quad \ldots$$
$$\#\tilde{E}_{\mathfrak{p}_{\ell-1}}(\mathbb{F}_{\mathfrak{p}_{\ell-1}}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_\ell), \quad \#\tilde{E}_{\mathfrak{p}_\ell}(\mathbb{F}_{\mathfrak{p}_\ell}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_1).$$

Many of the methods and results in this paper carry over in a straightforward manner to the number field case. For example, the following analogue of Theorem 13 holds.

Theorem 44. *Let $F/\mathbb{Q}$ be a number field, and let E/F be an elliptic curve with complex multiplication by an order in the quadratic imaginary field K. Suppose that $\mathfrak{p}$ and $\mathfrak{q}$ are degree one primes of F at*

which E has good reduction, that $\mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{p} \geq 5$*, and that*

$$\#\tilde{E}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) = \mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{q}.$$

Assume further that $j(E) \neq 0$. Then

$$\#\tilde{E}_{\mathfrak{q}}(\mathbb{F}_{\mathfrak{q}}) = \mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{p} \qquad \text{or} \qquad \#\tilde{E}_{\mathfrak{q}}(\mathbb{F}_{\mathfrak{q}}) = 2\,\mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{q} + 2 - \mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{p}.$$

It would be interesting to see to what extent the other results in this paper are valid over number fields, including especially the analysis of amicable pairs on curves with $j(E) = 0$.

Acknowledgements. The authors would like to thank Franz Lemmermeyer, Jonathan Wise, and Soroosh Yazdani for their assistance. The research in this note was performed while the first author was a long-term visiting researcher at Microsoft Research New England and included a short visit by the second author. Both authors thank MSR for its hospitality during their visits.

References

[1] T. M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[2] A. C. Cojocaru. Reductions of an elliptic curve with almost prime orders. *Acta Arith.*, 119(3):265–289, 2005.

[3] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[4] M. García, J. M. Pedersen, and H. te Riele. Amicable pairs, a survey. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 179–196. Amer. Math. Soc., Providence, RI, 2004.

[5] M. García, J. M. Pedersen, and H. te Riele. Amicable pairs, a survey. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 179–196. Amer. Math. Soc., Providence, RI, 2004.

[6] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[7] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[8] J. Jiménez Urroz. Almost prime orders of CM elliptic curves modulo p. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 74–87. Springer, Berlin, 2008.

[9] N. Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math.*, 131(1):157–165, 1988.

[10] S. Lang and H. Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in $\mathrm{G}L_2$-extensions of the rational numbers.

[11] F. Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.
[12] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.
[13] L. D. Olson. Hasse invariants and anomalous primes for elliptic curves with complex multiplication. *J. Number Theory*, 8(4):397–414, 1976.
[14] K. Rubin and A. Silverberg. Point counting on reductions of CM elliptic curves, 2009. `arXiv:0706.3711`.
[15] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.
[16] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comment. Math. Univ. St. Paul.*, 47(1):81–92, 1998.
[17] I. A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67(221):353–356, 1998.
[18] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.
[19] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
[20] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
[21] J. H. Silverman and K. E. Stange. Terms in an elliptic divisibility sequence divisible by their index. in preparation.
[22] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.
[23] C. Smyth. Lucas sequence terms divisible by their indices, 2009. `arXiv:0908.3832`.
[24] R. Taylor. Automorphy of some ℓ-adic lifts of automorphic mod ℓ representationsII, 2009. IHES Publ. Math., submitted for publication.
[25] H. J. J. te Riele. Perfect numbers and aliquot sequences. In *Computational methods in number theory, Part I*, volume 154 of *Math. Centre Tracts*, pages 141–157. Math. Centrum, Amsterdam, 1982.
[26] The PARI Group, Bordeaux. *PARI/GP, version* `2.3.4`, 2008. available from `http://pari.math.u-bordeaux.fr/`.
[27] W. C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.
[28] S. Y. Yan. *Perfect, amicable and sociable numbers*. World Scientific Publishing Co. Inc., River Edge, NJ, 1996. A computational approach.
[29] D. Zywina. A refinement of Koblitz's conjecture, 2009. `arXiv:0909.5280`.

Appendix A. Curves with $j = 0$ have no aliquot triples

In this section we use Corollary 24 and a detailed case-by-case analysis to show that an elliptic curve with $j = 0$ has no normalized aliquot triples (p, q, r) with $p > 7$. The details are sufficiently intricate that it

seems likely a different argument would be needed to prove that there are no aliqout cycles of length greater than three.

Proposition 45. *Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 0$. Then E has no normalized aliquot triples (p, q, r) with $p > 7$.*

Proof. We use Corollary 24, which says that if p and $q = \#\tilde{E}_p(\mathbb{F}_p)$ are prime, then $r = \#\tilde{E}_q(\mathbb{F}_q)$ takes one of six possible values. One of these six possible values is p, which is not allowed since we are assuming that p, q, r are distinct. Hence r has one of the following forms,

$$r = 2q + 2 - p, \qquad \text{(Case 1)}$$

$$r = \frac{\pm(q + 1 - p) \pm 3A_{p,q}}{2}, \qquad \text{(Case 2)}$$

where $A_{x,y}$ satisfies

$$A_{x,y}^2 = \frac{4xy - (x + y - 1)^2}{3}.$$

(Of course, Case 2 is really four cases, depending on the choice of signs.)

For the moment letting $s = \#\tilde{E}_r(\mathbb{F}_r)$, we can apply the same reasoning to (q, r, s) to deduce that

$$s = 2r + 2 - q, \qquad \text{(Case A)}$$

$$s = \frac{\pm(r + 1 - q) \pm 3A_{q,r}}{2}. \qquad \text{(Case B)}$$

To ease notation, we let

$$F(x, y) = \frac{\pm(y + 1 - x) \pm 3A_{x,y}}{2}.$$

Then the two cases for r followed by the two cases for s give four possibilities for s in terms of p and q:

$$s = 3q + 6 - 2p, \qquad \text{(Case 1A)}$$

$$s = 2F(p, q) + 2 - q, \qquad \text{(Case 2A)}$$

$$s = F(q, 2q + 2 - p), \qquad \text{(Case 1B)}$$

$$s = F\big(q, F(p, q)\big). \qquad \text{(Case 2B)}$$

(Of course, each case is really several cases depending on the choice of signs for each occurrence of F.)

The assumption that (p, q, r) is an aliquot triple is equivalent to saying that $s = p$. Suppose first we are in Case 1A. Then $s = p$ is equivalent to

$$3q + 6 - 2p = p,$$

so $p = q+2$. This contradicts our assumption that the triple is normalized, i.e., that p is the smallest element of the triple. Hence Case 1A is not possible.

Next we consider Case 2A. Then the assumption $s = p$ implies that $2F(p,q) = p+q-2$. Using the definition of F, this can be written as

$$\pm(q+1-p) \pm 3A_{p,q} = p+q-2,$$

which (using the definition of A) implies that

$$\big((p+q-2) \pm (q+1-p)\big)^2 = 9A_{p,q}^2 = 3\big(4pq - (p+q-1)^2\big). \quad (42)$$

This gives two subcases, which we denote by $2A^+$ and $2A^-$ according to the choice of sign. A little bit of algebra yields

$$28p^2 - 24pq + 12q^2 - 72p - 24q + 48 = 0, \qquad (\text{Case } 2A^+)$$
$$12p^2 - 24pq + 28q^2 - 24p - 40q + 16 = 0. \qquad (\text{Case } 2A^-)$$

Both of the functions on the left-hand sides have leading quadratic forms that are positive definite, so there are only finitely many integral solutions (p,q). A more careful analysis shows that the first is positive for $p > 5$ and the second is positive for $p > 7$.

Next comes Case 1B, where the assumption that $s = p$ leads to the formula

$$F(q, 2q+2-p) = p.$$

Writing this out in terms of $A_{q,2q+2-p}$, moving all the other terms to the other side, squaring, and simplifying, we again get two cases depending a choice of sign. Thus

$$12p^2 - 12pq + 4q^2 - 24p + 12 = 0, \qquad (\text{Case } 1B^+)$$
$$4p^2 - 4pq + 4q^2 + 12 = 0. \qquad (\text{Case } 1B^-)$$

The quadratic function for Case $1B^+$ is positive for $p > 7$ and the quadratic function for Case $1B^-$ is positive for $p > 0$.

Finally we turn to Case 2B, which is somewhat more complicated because it is given by the formula

$$F\big(q, F(p,q)\big) = p,$$

which involves two iterations of the function F. The signs on the $A_{x,y}$ terms are irrelevant since we square them, but the other signs in the definition of F do affect the eventual equation. After a bunch of algebra, we find that the p and q values for an amicable triple coming from Case 2B must satisfy one of the following equations.

$$4p^4 + 2p^3q + 3p^2q^2 - pq^3 + q^4 - 6p^3 - 15p^2q$$
$$- 15pq^2 + 3p^2 + 3pq + 3q^2 = 0 \quad (\text{Case } 2B^{++})$$

$$\begin{aligned} 9p^2q^2 - 9pq^3 + 9q^4 + 9p^2q - 27pq^2 + 3p^2 - 21pq \\ - 3q^2 - 6p + 6q + 4 = 0 \quad \text{(Case } 2\text{B}^{+-}\text{)} \\ 3p^2q^2 - 3pq^3 + q^4 + 9p^2q - 9pq^2 + 9p^2 - 9pq + 3q^2 = 0 \quad \text{(Case } 2\text{B}^{-+}\text{)} \\ 4p^4 - 18p^3q + 33p^2q^2 - 27pq^3 + 9q^4 - 10p^3 + 33p^2q \\ - 21pq^2 + 21p^2 - 21pq - 3q^2 - 10p + 6q + 4 = 0 \quad \text{(Case } 2\text{B}^{--}\text{)} \end{aligned}$$

All of these quartic functions are positive if $0 < p < q$ with p sufficiently large. More precisely, it suffices to take $p > 3$ for Cases 2B^{++} and 2B^{+-}, $p > 4$ for Case 2B^{-+} and $p > 2$ for Case 2B^{--}.

This completes the proof that E has no aliquot triples. □

Appendix B. Proof of independence of the maps in Proposition 34

We give a proof for $\mathrm{char}(\mathbb{F}) = 0$. Independence of maps is geometric, so it suffices to prove independence for $\gamma = \delta = 1$. Let $\psi_1, \ldots, \psi_4$ be the four maps in Proposition 34(b), so

$$\begin{aligned} \psi_1 &: C_6^{(1,1)} \longrightarrow E^{(16)}, & \psi_2 &: C_6^{(1,1)} \longrightarrow E^{(4)}, \\ \psi_3 &: C_6^{(1,1)} \longrightarrow E^{(1)}, & \psi_4 &: C_6^{(1,1)} \longrightarrow E^{(-1)}. \end{aligned}$$

We compose these maps with untwisting maps $E^{(\kappa)} \to E^{(1)}$, so we get four maps

$$\begin{aligned} \phi_1 &: C_6^{(1,1)} \xrightarrow{\psi_1} E^{(16)} \xrightarrow{(x,y)\to\left(\frac{1}{2\sqrt[3]{2}}x, \frac{1}{4}y\right)} E^{(1)}, \\ \phi_2 &: C_6^{(1,1)} \xrightarrow{\psi_2} E^{(4)} \xrightarrow{(x,y)\to\left(\frac{1}{\sqrt[3]{4}}x, \frac{1}{2}y\right)} E^{(1)}, \\ \phi_3 &: C_6^{(1,1)} \xrightarrow{\psi_3} E^{(1)} \xrightarrow{(x,y)\to(x,y)} E^{(1)}, \\ \phi_4 &: C_6^{(1,1)} \xrightarrow{\psi_4} E^{(-1)} \xrightarrow{(x,y)\to(-x,iy)} E^{(1)}. \end{aligned}$$

The maps $\psi_1, \ldots, \psi_4$ are defined over $\mathbb{Q}$, but the maps $\phi_1, \ldots, \phi_4$ are only defined over $\bar{\mathbb{Q}}$, not $\mathbb{Q}$. We consider the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on these maps. To do this, we choose elements $\sigma, \tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ satisfying

$$\begin{aligned} \sigma(\sqrt[3]{2}) &= \rho\sqrt[3]{2}, & \sigma(i) &= i, \\ \tau(\sqrt[3]{2}) &= \sqrt[3]{2}, & \tau(i) &= -i. \end{aligned}$$

Here $\rho = \frac{1}{2}(-1 + \sqrt{-3})$ is a fixed primitive cube root of unity. We also note that $\boldsymbol{\mu}_3$ acts on $E^{(1)}$ via $[\rho](x, y) = (\rho x, y)$. Looking at the

explicit formulas for $\phi_1, \dots, \phi_4$, we find that

$$\begin{aligned} \phi_1^\sigma &= [\rho^2] \circ \phi_1, & \phi_2^\sigma &= [\rho] \circ \phi_2, & \phi_3^\sigma &= \phi_3, & \phi_4^\sigma &= \phi_4, \\ \phi_1^\tau &= \phi_1, & \phi_2^\tau &= \phi_2, & \phi_3^\tau &= \phi_3, & \phi_4^\tau &= [-1] \circ \phi_4. \end{aligned}$$

Now suppose that we have a relation

$$[n_1] \circ \phi_1 + [n_2] \circ \phi_2 + [n_3] \circ \phi_3 + [n_4] \circ \phi_4 = 0. \tag{43}$$

Applying the transformation τ to (43) has the effect of replacing ϕ_4 by $[-1] \circ \phi_4$, so subtracting the two equations yields $[2n_4] \circ \phi_4 = 0$. Since the map $\phi_4 : C_6^{(1,1)} \to E^{(1)}$ is a finite map, it follows that $n_4 = 0$.

Applying σ and σ^2 to (43), we end up with three equations

$$[n_1] \circ \phi_1 + [n_2] \circ \phi_2 + [n_3] \circ \phi_3 = 0, \tag{44}$$

$$[n_1] \circ [\rho^2] \circ \phi_1 + [n_2] \circ [\rho] \circ \phi_2 + [n_3] \circ \phi_3 = 0, \tag{45}$$

$$[n_1] \circ [\rho] \circ \phi_1 + [n_2] \circ [\rho^2] \circ \phi_2 + [n_3] \circ \phi_3 = 0. \tag{46}$$

Adding (44), (45), and(46) and using $1+\rho+\rho^2 = 0$ gives $[3n_3] \circ \phi_3 = 0$, which implies that $n_3 = 0$. Similarly, adding (44) to $[\rho]$ times (45) to $[\rho^2]$ times (46) gives $[3n_1] \circ \phi_1 = 0$, so $n_1 = 0$. Finally, since $n_1 = n_3 = 0$, the equation (44) gives $n_2 = 0$. This completes the proof that $\phi_1, \dots, \phi_4$ are independent.

Appendix C. Evaluating the formula for $M_k^{[1]}$ when $k \equiv 1 \pmod 3$

In this appendix we give the PARI [26] script that we used to compute $M_k^{[1]}(S, 1)$ via the formulas (36), (37), (38), and (39). In these formulas we treat k, π, and ϵ as indeterminates and formally set $\bar{\pi} = k/\pi$ and $\bar{\epsilon} = 1/\epsilon$. The value of $M_k^{[1]}(S, 1)$ turns out to be independent of k mod 4 and is always a quadratic polynomial in k. The output from the routine `TestFormulaForSplitPrimes` is given in Table 8, which was calculated using the following PARI program.

```
/* The function TestFormulaForSplitPrimes computes M_k^{[1]}
   for k = 1 (mod 3), using the formula as a sum of products of #C - e terms.
   The following global variables must be left as indeterminates:
   k, pi, e2
   Here e2 represents the cubic residue of 2 modulo pi.
   The conjugates of these are given by
   pibar = k/pi  and   e2bar = 1/e2.
   Further, w is assigned the value quadgen(-3), and wbar = conj(w) = 1/w
*/

{
TestFormulaForSplitPrimes() =
  local(m,ISets,IndexSet);
  print("\\begin{align*}");
  forstep(kmod4 = 1, 3, 2,
```

$$
\begin{aligned}
&k \equiv 1 \pmod 4\\
&\#M_k^{[1]}(\omega^0,1) = (1/18)(k^2+4k+13)\\
&\#M_k^{[1]}(\omega^1,1) = (1/18)(k^2-2k+1)\\
&\#M_k^{[1]}(\omega^2,1) = (1/18)(k^2-2k+1)\\
&\#M_k^{[1]}(\omega^3,1) = (1/18)(k^2-8k+7)\\
&\#M_k^{[1]}(\omega^4,1) = (1/18)(k^2-2k+1)\\
&\#M_k^{[1]}(\omega^5,1) = (1/18)(k^2-2k+1)
\end{aligned}
$$

$$
\begin{aligned}
&k \equiv 3 \pmod 4\\
&\#M_k^{[1]}(\omega^0,1) = (1/18)(k^2+4k+13)\\
&\#M_k^{[1]}(\omega^1,1) = (1/18)(k^2-2k+1)\\
&\#M_k^{[1]}(\omega^2,1) = (1/18)(k^2-2k+1)\\
&\#M_k^{[1]}(\omega^3,1) = (1/18)(k^2-8k+7)\\
&\#M_k^{[1]}(\omega^4,1) = (1/18)(k^2-2k+1)\\
&\#M_k^{[1]}(\omega^5,1) = (1/18)(k^2-2k+1)
\end{aligned}
$$

$$
\begin{aligned}
\#M_k^{[1]}\big(\{\omega^1,\omega^5\},1\big) &= (1/9)(k^2-2k+1)\\
\#M_k^{[1]}\big(\{\omega^1,\omega^3,\omega^5\},1\big) &= (1/6)(k^2-4k+3)\\
\#M_k^{[1]}\big(\{\omega^1,\omega^2,\omega^4,\omega^5\},1\big) &= (2/9)(k^2-2k+1)\\
\#M_k^{[1]}\big(\{\omega^0,\omega^1,\omega^2,\omega^3,\omega^4,\omega^5\},1\big) &= (1/3)(k^2-2k+4)
\end{aligned}
$$

TABLE 8. Results of computing of $M_k^{[1]}(S,1)$ using PARI

```
  print("  k\\equiv ",kmod4," \\pmod{4} \\\\");
  for (i = 0, 5,
    m = MMSum([i],kmod4);
    print1("  \\#M_k^{[1]}(\\o^",i,",1) &= ");
    print1("(",content(content(m)),")(",m/content(content(m)),")");
    if (i < 5 || kmod4 == 1, print(" \\\\"), print);
  );
  if (kmod4 == 1, print("  \\\\"));
);
print("\\end{align*}");
print("\\begin{align*}");
ISets = [[1,5], [1,3,5], [1,2,4,5], [0,1,2,3,4,5]];
for (j = 1, #ISets,
  IndexSet = ISets[j];
```

```
    m = MMSum(IndexSet,1);
    print1("  \\#M_k^{[1]}\\bigl(\\{");
    for (i = 1, #IndexSet,
      print1("\\o^",IndexSet[i]);
      if (i < #IndexSet, print1(","));
    );
    print1("\\},1\\bigr)\n     &= (",content(content(m)),")");
    print1("(",m/content(content(m)),")");
    if (j < #ISets, print(" \\\\"), print);
  );
  print("\\end{align*}");
}

w = quadgen(-3);
wbar = conj(w);
pibar = k/pi;
e2bar = 1/e2;

{
CC(u,v,kmod4) =
  if (kmod4 == 0, error("k mod 4 must be 1 or 3"));
  k + 1
     + w^(2*v)*pibar + wbar^(2*v)*pi
     + e2^2*w^(3*u+4*v)*pibar + e2bar^2*wbar^(3*u+4*v)*pi
     + e2*w^(5*u+2*v)*pibar + e2bar*wbar^(5*u+2*v)*pi
     + (-1)^((kmod4-1)/2)*e2*w^(u+2*v)*pibar
     + (-1)^((kmod4-1)/2)*e2bar*wbar^(u+2*v)*pi;
}

{
ee(u,v) =
  if (u % 6 == 0, 6, 0)
    + if((u-v) % 3 == 0, 3, 0)  + if((2*u-v) % 3 == 0, 3, 0);
}

MM(u,v,kmod4) = (1/18) * (CC(u,v,kmod4) - ee(u,v));

{
MMSum(IndexSet,kmod4) =
  local(i,s);
  s = 0;
  for (j = 1, #IndexSet,
    i = IndexSet[j];
    for (u = 0, 5,
    for (v = 0, 2,
      s = s + MM(u,v,kmod4)*MM(u-i,v,kmod4);
    );
    );
  );
  return(s);
}
```

Appendix D. Amicable pairs for $y^2 + y = x^3 + x^2$ up to 10^{11}

We used PARI-GP [26] to compute all normalized amicable pairs (p, q) on the curve $y^2 + y = x^3 + x^2$ with $p < 10^{11}$. The list is given in Table 9.

(853,883)	(77761,77999)
(1147339,1148359)	(1447429,1447561)
(82459561,82471789)	(109165543,109180121)
(253185307,253194619)	(320064601,320079131)
(794563993,794571803)	(797046407,797057473)
(2185447367,2185504261)	(2382994403,2383029443)
(4101180511,4101190039)	(4686466159,4686510971)
(5293671709,5293749623)	(6677602471,6677694539)
(7074693823,7074704971)	(7806306133,7806380963)
(9395537549,9395559011)	(9771430993,9771433303)
(9849225103,9849306373)	(10574564857,10574619851)
(12657210407,12657303353)	(13003880317,13003900901)
(13789895011,13790023199)	(14436076927,14436180091)
(14976551207,14976590371)	(15597047659,15597075937)
(15679549877,15679688491)	(16322301811,16322366867)
(17725049203,17725142719)	(17841395323,17841406601)
(31615097957,31615194739)	(33266376239,33266419807)
(33963999907,33964128017)	(34525477799,34525684639)
(39287748091,39287808559)	(40136806357,40137038941)
(46438194193,46438453213)	(51838270219,51838493561)
(51881025571,51881167549)	(52011956957,52012184953)
(55823622193,55823919169)	(57920520199,57920640709)
(62765305697,62765625749)	(62995853671,62996152237)
(66252308051,66252349753)	(67177409329,67177631771)
(69449506103,69449741239)	(75002612911,75002660263)
(77264683829,77264993327)	(77635421531,77635670141)
(79067605783,79067881429)	(81263083703,81263204563)
(94248260597,94248586591)	

TABLE 9. Amicable pairs for $y^2 + y = x^3 + x^2$ up to 10^{11}

MATHEMATICS DEPARTMENT, BOX 1917, BROWN UNIVERSITY, PROVIDENCE, RI 02912 USA

E-mail address: jhs@math.brown.edu

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, 8888 UNIVERSITY DRIVE, BURNABY, BC, CANADA V5A 1S6, AND PACIFIC INSTITUTE FOR THE MATHEMATICAL SCIENCES, 200 1933 WEST MALL, VANCOUVER, BC, CANADA V6T 1Z2

E-mail address: kestange@pims.math.ca